Stanford Law Review

Volume 74 April 2022

NOTE

Digital Eyewitnesses: Using New Technologies to Authenticate Evidence in Human Rights Litigation

Bailey R. Ulbricht, Christopher Moxley,
Mackenzie D. Austin & Molly D. Norburg*

Abstract. Human rights abuses are increasingly documented through smartphones and personal cameras, generating hundreds of terabytes of digital content from Idlib to Minneapolis. While digital evidence provides an important opportunity to democratize the documentation of abuses, the quantity and diversity of this data present challenges for those seeking accountability. Legal advocates must find ways to safely store digital content, parry attempts at manipulation or corruption, and eventually ensure authentication before a court of law. Should litigation arise, the individual who created the digital record is often unreachable or otherwise unavailable to testify, further complicating the underlying legal questions. NGOs and legal advocates have increasingly adopted two new tools—cryptographic hashing and distributed-ledger technology (DLT)—to clear these hurdles. In addition to imbuing civilian-generated evidence with a greater sense of legitimacy and providing immutable protection, these technologies help human rights documentation satisfy U.S. standards for admissibility of evidence.

Existing legal scholarship has neither examined these technologies as they relate to U.S. authentication standards nor scrutinized whether they support authentication without witness testimony. There is also a dearth of scholarship that (1) deconstructs and explains these technologies for a legal audience; and (2) provides specific recommendations for courts and litigants. This Note fills these gaps by arguing that, with or without witness testimony, these technologies can support the authentication of digital evidence under U.S.

[*] J.D. Candidates, Stanford Law School, 2022. We owe our deepest gratitude to Professor Beth Van Schaack for her invaluable guidance, as well as to the members of the Fall 2020 Stanford Human Rights & International Justice Policy Practicum for their support. We are indebted to Jonathan Dotan, Stephen Honan, Lindsay Freeman, Riana Pfefferkorn, David Alan Sklansky, and David Freeman Engstrom for feedback during the research and drafting process. Thanks also to our peers on the *Stanford Law Review*—Konadu Amoakuh, Kylie Choi, Olivia Goldberg, Chris Huberty, Hannah Hunt, Daniel Khalessi, Matt Krantz, David Levin, Marisa Lowe, and Grace Rehaut—for their incisive edits. We reserve our greatest admiration for the human rights practitioners testing digital strategies in the field, along with those risking their lives every day to collect evidence of human rights abuses.

statutory and common law requirements. In doing so, it creates a roadmap for how cases that rely on digital evidence can proceed in U.S. courts. Ideally, this roadmap will help to democratize accountability by facilitating new opportunities for justice where admissibility issues previously foreclosed litigation.

Table of Contents

Introduction

On October 7, 2020, the Department of Justice announced the indictment of two former British citizens suspected of membership in an infamous Islamic State of Iraq and Syria (ISIS) trafficking cell known as "The Beatles."[1] Defendants Alexanda Amon Kotey and El Shafee Elsheikh had allegedly participated in the kidnapping, torture, and murder of civilian hostages, including four American citizens, in Syria from 2012 to 2015.[2] Because the Department of Justice struggled to access physical evidence, the indictment cited emails to the victims' families coordinating ransom negotiations—combined with voice memos, images of beheadings, and audio that the hostages were forced to record—to piece together the suspects' roles in ISIS.[3] The evidence used in this case reflects a broader trend in human rights and international criminal litigation: In pursuit of accountability, prosecutors are leaning on digital evidence in lieu of traditional evidentiary sources such as live witness testimony.[4]

But the increasing reliance on digital documentation in human rights settings is brushing up against the constraints of evidence law. To prevent unsubstantiated evidence from reaching the trier of fact, the U.S. legal system requires evidence to be authenticated before it can be admitted.[5] For an item of evidence to be authenticated, its proponent must produce sufficient additional evidence to establish that "the item is what the proponent claims it is."[6] For digital evidence, this supporting proof can take the form of testimony from individuals with personal knowledge regarding the creation of the digital object. The author of an email, for example, can vouch for its authenticity.[7] The authentication requirement poses acute challenges in human rights litigation, because crimes committed on battlefields abroad often do not

[1] Press Release, U.S. Att'y's Off. for the E. Dist. of Virginia, U.S. Dep't of Just., ISIS Militants Charged with Deaths of Americans in Syria (updated Oct. 7, 2020), https://perma.cc/E5BV-WGWQ.

[2] *Id.* Kotey has since pleaded guilty. Press Release, U.S. Dep't of Just., ISIS Militant Pleads Guilty to Role in Deaths of Four Americans in Syria (updated Sept. 30, 2021), https://perma.cc/NM5M-GJFV.

[3] *See* Indictment ¶¶ 7, 39-42, 44, United States v. Kotey, No. 20-cr-00239 (E.D. Va. Oct. 6, 2020), ECF No. 1.

[4] *See* Aisling Irwin, *Digital Evidence Opens Doors to Human Rights Probes*, SCIDEV.NET (Mar. 20, 2019), https://perma.cc/Y75P-JHNB (documenting the rise of digital evidence in human rights litigation and identifying efforts by NGOs to train digital evidence collectors).

[5] *See* FED. R. EVID. 901(a).

[6] *Id.*

[7] Michaela Battista Sozio, *Authenticating Digital Evidence at Trial*, A.B.A.: BUS. L. TODAY (Apr. 27, 2017), https://perma.cc/WUU7-MKV3.

generate readily accessible witness testimony or physical evidence to authenticate the digital record. Indeed, the challenge of introducing admissible evidence of human rights violations has thwarted efforts by the United States and its allies to prosecute foreign fighters.[8] Testifying before the Senate Foreign Relations Committee, violent-extremism expert Lorenzo Vidino explained that as of 2017, only 54 of the 400 British foreign fighters "known to have returned back from Syria and Iraq" had been convicted—in large part due to a "lack of actionable evidence."[9]

The difficulties facing the prosecution in the Kotey and Elsheikh case are shared by many who seek to hold human rights abusers accountable. Governments, human rights NGOs, and individuals have collected mountains of digital evidence documenting abuses taking place all over the world, from war crimes in Syria to violence against Black Lives Matter protestors in Washington, D.C.[10] At the same time, finding live witness testimony to authenticate digital evidence is challenging. For a particular incident, there may be no surviving witnesses, no logistically accessible witnesses, or no witnesses who can safely testify without reprisal.[11] Thus, in today's accountability proceedings, digital evidence—including communications, data, video, and images—often serves as the only "eyewitness" shining light on human rights abuses.[12] Yet the U.S. legal system has lagged behind in adapting evidence law to address the realities of the digital age. Courts continue to prioritize witness testimony, even when evaluating the admissibility of evidence generated by mechanistic processes.[13]

There is an emerging need in legal scholarship to explore how human rights violations are prosecuted when digital evidence predominates. Although the benefits of digital tools are becoming widely recognized in the human rights space,[14] little has been written about whether and how digital evidence

[8] *Beyond Iraq and Syria: ISIS' Global Reach: Hearing Before the S. Comm. on Foreign Rels.*, 115th Cong. 4 (2017) (statement of Lorenzo Vidino, Director, Program on Extremism, George Washington University).

[9] *Id.*

[10] *See infra* Part I.

[11] *See* Daniela Gavshon & Emily Rice, *International Human Rights Fact-Finding in Hostile Environments: Guidelines for Interviewing in Restricted Access Contexts*, JUST SEC. (Oct. 1, 2021), https://perma.cc/2EED-YZCC; *infra* note 93 and accompanying text.

[12] *See* Irwin, *supra* note 4.

[13] Edward K. Cheng & G. Alexander Nunn, *Beyond the Witness: Bringing a Process Perspective to Modern Evidence Law*, 97 TEX. L. REV. 1077, 1092 (2019).

[14] *See, e.g.*, Hum. Rts. Ctr., Univ. of Cal., Berkeley, Sch. of L. & Off. of the U.N. High Comm'r for Hum. Rts., *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*, at v-vii, U.N. Doc. HR/PUB/20/2 (advance version 2020) [hereinafter *Berkeley Protocol*],

footnote continued on next page

can be admitted in formal accountability proceedings. Some scholarship has questioned whether witnesses should be required for authentication, arguing instead that authentication should focus on the process of collection,[15] which could better leverage new technologies. Other scholarship has discussed the influence of technology on the legal system generally.[16] But little scholarship has analyzed digital tools in the litigation context. And no scholarship has assessed whether cryptographic hashing and distributed-ledger technology (DLT) satisfy authentication requirements or provided recommendations for courts using these tools.

This Note fills these gaps by analyzing how hashing and DLT can safeguard digital evidence and facilitate its admissibility under U.S. law. In doing so, the Note emphasizes, these technologies can democratize accountability by supplementing the record when a dearth of available witnesses threatens to undermine efforts to achieve justice. Though these technologies have the potential to be used in jurisdictions around the world, we focus on the United States, which has stricter admissibility rules than most civil law systems.[17]

The Note proceeds as follows. Part I provides background on the current challenges facing human rights documentation. Part II defines and outlines the key features of hashing and DLT. Part III then explores the potential for these technologies to facilitate the authentication (and thus the admission) of digital evidence. It also considers potential problems with the widespread use of digital evidence given the benefits of witness testimony. In light of this analysis, Part IV offers recommendations for how U.S. courts should approach digital evidence that relies on cryptography and DLT for authentication.

I. Evolution of Human Rights Documentation

The importance of preserving and authenticating records of human rights violations is not new to the digital age. In the aftermath of World War II, the prosecution of Nazi leadership at the International Military Tribunal at

https://perma.cc/SFZ5-7NHL (recognizing the ubiquity of digital evidence and offering a set of best practices for using the internet to investigate human rights abuses).

[15] *See* Cheng & Nunn, *supra* note 13, at 1078-82.

[16] *See, e.g.*, David Freeman Engstrom & Jonah B. Gelbach, *Legal Tech, Civil Procedure, and the Future of Adversarialism*, 169 U. PA. L. REV. 1001, 1008-09 (2021) (discussing how technology might affect the legal system).

[17] *See* Caslav Pejovic, *Civil Law and Common Law: Two Different Paths Leading to the Same Goal*, 32 VICTORIA U. WELLINGTON L. REV. 817, 832-33 (2001) (explaining that common law systems contain "several rules which restrict admission of evidence," while generally in civil law systems "any evidence is admissible, but the court will evaluate how much weight [it] is to be accorded").

Nuremberg relied on the regime's detailed physical records of its operations, which had been seized by Allied forces.[18] Accordingly, some defendants sought to undermine the credibility of documents that were unsigned or misdated.[19] In response, the tribunal looked to the meticulous preparation and preservation of the documents to establish "their authenticity and substantial truth."[20] The prosecution supplemented documentary evidence with recordings of, for example, mass graves captured on film by Allied forces.[21] This "[g]rim evidence of mass murder[]" powerfully substantiated the atrocities outlined in the written documents.[22]

The ensuing convictions predicated on the records and footage proved that detailed, secure documentation of human rights abuses can serve as a foundation for accountability.[23] In the same era, the Universal Declaration of Human Rights and the U.N. Charter articulated novel human rights principles "as a common standard of achievement for all peoples and all nations."[24] Responses to the atrocities committed during World War II thus projected the aspirational (if oft-unfulfilled) message that it was unacceptable to deny individuals the enjoyment of certain fundamental rights, and that individuals could achieve some redress by documenting violations of those rights.

In the postwar period, the steady development of international institutions and rapid advances in technology increased the breadth and sophistication of human rights abuse documentation. On the legal side, the international community began to establish more robust bodies to enforce human rights protections. The U.N. created its Commission on Human Rights

[18] *See* 22 TRIAL OF THE MAJOR WAR CRIMINALS BEFORE THE INTERNATIONAL MILITARY TRIBUNAL 413 (1948) ("The case, therefore, against the defendants rests in a large measure on documents of their own making . . . .").

[19] *Id.* at 429 (noting that documents describing certain meetings had "been subject to some criticism at the hands of defending counsel" due to inconsistencies in signature, date, and content).

[20] *Id.*

[21] *Id.* at 494.

[22] *Id.*; *see also* CHRISTIAN DELAGE, CAUGHT ON CAMERA: FILM IN THE COURTROOM FROM THE NUREMBERG TRIALS TO THE TRIALS OF THE KHMER ROUGE 63 (Ralph Schoolcraft & Mary Byrd Kelly eds. & trans., Univ. of Pa. Press 2014) (2006) (detailing the role of film footage in motivating the United States to prosecute the Nazis).

[23] *See* Lindsay Freeman, *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, 41 FORDHAM INT'L L.J. 283, 299 (2018) ("Justice Jackson demonstrated an important truth: that despite the grave and horrific nature of the crimes, a criminal case could be successful based on cold, hard facts and evidence . . . .").

[24] G.A. Res. 217 (III) A, Universal Declaration of Human Rights, pmbl. (Dec. 10, 1948); U.N. Charter pmbl.

in 1946,[25] and regional bodies followed.[26] Tribunals were established to prosecute grave violations of fundamental rights, first on an ad hoc basis (to address conflicts like those in the former Yugoslavia and Rwanda) and later on a permanent basis with the formation of the International Criminal Court (ICC).[27] Meanwhile, countries ratified core human rights treaties, accepting obligations to provide domestic redress for human rights violations.[28] Taking advantage of these new forums for human rights claims, civil-society groups documenting human rights violations also proliferated—including Amnesty International, founded in 1961,[29] and Human Rights Watch, founded in 1978.[30] Throughout the latter half of the twentieth century, civilians, journalists, and civil-society groups worldwide kept physical records of human rights abuses in the pursuit of justice.[31]

In the new millennium, the advent of the digital age transformed the process of human rights documentation, allowing anyone with a cell phone to record human rights violations and anyone with internet access to broadcast content to the world. These developments helped to propel movements like the Arab Spring across national boundaries.[32] Perhaps no conflict better demonstrates this evolution than the civil war in Syria, where digital evidence has been instrumental in alerting the international community to violations of

[25] *HR Commission Archives: Introduction*, UNITED NATIONS HUM. RTS. COUNCIL, https://perma.cc/GL97-75GU (archived Dec. 30, 2021). The U.N. Human Rights Council replaced the U.N. Commission on Human Rights in 2006. *Welcome to the Human Rights Council*, UNITED NATIONS HUM. RTS. COUNCIL, https://perma.cc/JA54-YQSC (archived Apr. 16, 2022).

[26] Convention for the Protection of Human Rights and Fundamental Freedoms art. 19, Nov. 4, 1950, 213 U.N.T.S. 221 (European); American Convention on Human Rights art. 33, Nov. 22, 1969, 1144 U.N.T.S. 123 (Inter-American).

[27] *See* S.C. Res. 827, ¶ 2 (May 25, 1993); S.C. Res. 955, ¶ 1 (Nov. 8, 1994); Rome Statute of the International Criminal Court art. 1, July 17, 1998, 2187 U.N.T.S. 90.

[28] *See, e.g.*, Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment art. 14, ¶ 1, Dec. 10, 1984, 108 Stat. 382, 1465 U.N.T.S. 85 ("Each State Party shall ensure in its legal system that the victim of an act of torture obtains redress and has an enforceable right to fair and adequate compensation . . . .").

[29] *Who We Are*, AMNESTY INT'L, https://perma.cc/HUL6-7WM3 (archived Dec. 30, 2021).

[30] *About Us*, HUM. RTS. WATCH, https://perma.cc/2KSH-TCUQ (archived Dec. 30, 2021).

[31] For example, the Genocide Archive of Rwanda maintains a physical collection of artifacts from the Rwandan genocide in 1994. *Physical Preservation*, GENOCIDE ARCHIVE RWANDA, https://perma.cc/57NN-JV73 (archived Dec. 30, 2021). For a history of efforts to archive evidence of conflict since World War II, see generally ARCHIVES AND HUMAN RIGHTS (Jens Boel, Perrine Canavaggio & Antonio González Quintana eds., 2021).

[32] *See* Catherine O'Donnell, *New Study Quantifies Use of Social Media in Arab Spring*, UNIV. WASH.: UW NEWS (Sept. 12, 2011), https://perma.cc/U6WG-38A5.

human rights law and international humanitarian law.[33] In fact, there are "more hours of footage of the Syrian civil war on YouTube then [sic] there actually are hours of the war in real life."[34]

The democratization of human rights abuse documentation is not limited to armed-conflict zones. In the United States, the Black Lives Matter movement made extensive use of video in the protests following the murder of George Floyd, to both publicize the movement's message and allow investigators to identify and verify acts of violence by police officers.[35] Across a range of substantive issues, NGOs have developed tools to collect, store, and disseminate digital evidence,[36] while domestic legal systems and international tribunals have adopted protocols codifying best practices for submitting digital evidence to courts.[37] In the aftermath of World War II, Allied forces searched for centralized Nazi records, finding them "in salt mines, buried in the ground, [and] hidden behind false walls and in other places thought to be secure from discovery."[38] Today, individuals generate their own digital records of human rights violations in real time and disseminate and store that evidence across borders via the internet.

Despite the benefits of digital evidence, its proliferation has raised challenges in each phase of the evidentiary life cycle. These challenges are significant, and they sometimes threaten to undermine the ultimate determination of admissibility. For example, at the storage phase, securely preserving countless hours of film footage or thousands of photos for years is a monumental logistical challenge. Additionally, retaining proof of human rights violations can entail serious risks: Government forces have tortured and

[33] *See, e.g.*, *How Open Source Evidence Took a Lead Role in the Response to the Douma Chemical Weapons Attack*, AMNESTY INT'L (Apr. 23, 2018, 11:21 AM), https://perma.cc/LVJ4-ERUV.

[34] Armin Rosen, *Erasing History: YouTube's Deletion of Syria War Videos Concerns Human Rights Groups*, FAST CO. (Mar. 7, 2018) (quoting Google product manager Justin Kosslyn), https://perma.cc/G639-9CA6.

[35] *See* Heather Kelly & Rachel Lerman, *America is Awash in Cameras, a Double-Edged Sword for Protestors and Police*, WASH. POST (June 3, 2020), https://perma.cc/JV8P-Q7UD. Technology cuts both ways in this context, as police can also use video to identify protestors. *Id.*

[36] *See, e.g.*, Irwin, *supra* note 4.

[37] *See, e.g.*, INT'L CRIM. CT., ICC-01/14-01/18-64-ANX, UNIFIED TECHNICAL PROTOCOL ("E-COURT PROTOCOL") FOR THE PROVISION OF EVIDENCE, WITNESS AND VICTIMS INFORMATION IN ELECTRONIC FORM 1 (2019), https://perma.cc/VU5W-LBTN; NAT'L INST. OF JUST., U.S. DEP'T OF JUST., NCJ NO. 211314, DIGITAL EVIDENCE IN THE COURTROOM: A GUIDE FOR LAW ENFORCEMENT AND PROSECUTORS, at iii (2007), https://perma.cc/AQ98-V4HW.

[38] 22 TRIAL OF THE MAJOR WAR CRIMINALS BEFORE THE INTERNATIONAL MILITARY TRIBUNAL, *supra* note 18, at 413.

killed civilians in Syria over the contents of their phones.[39] Individuals and civil-society organizations have published videos of human rights violations on YouTube to create an internet record, only for thousands of those videos to be taken down by YouTube's content-moderation algorithms, complicating efforts to pin down an original, authentic source.[40] These issues at the storage stage are compounded by struggles to find witnesses who can attest to the authenticity of stored evidence, especially given that proceedings often take place years after events and in far-off jurisdictions. Though it is best to involve witnesses in accountability proceedings whenever possible, the international legal community should explore ways to guarantee safe storage so that digital evidence can be authenticated when live testimony is sparse.

II. The Emergence of Safe-Storage Technologies

Before applying cryptographic hashing and DLT to existing standards for authenticating evidence, it is critical to clarify how these technologies work. Part II.A provides a brief explanation of the technical aspects of hashing and DLT and describes how these technologies operate to protect digital records. Part II.B then details how human rights organizations are currently leveraging hashing and DLT and discusses other potential applications.

Two acknowledgements must be made at the outset. First, while these technologies are relatively novel in the human rights space, hashing and DLT have started to achieve widespread adoption by corporate actors.[41] Much has been written about the potential of blockchain technology—a form of DLT—to revolutionize a variety of sectors, from entrepreneurship to energy to elections.[42] Second, these technologies do not account for the first stage in the digital evidence life cycle: the moment of creation and means of collection. What happens at the collection stage is critical to later efforts at verification, and the collection stage presents a different universe of legal vulnerabilities, which we briefly address in Part III.E. While others have begun to examine the

[39] Deirdre Collings & Robert Muggah, *Digital Safety in the World's Most Dangerous War Zone*, IGARAPÉ INST. (Apr. 27, 2018), https://perma.cc/LA88-24RH.

[40] Malachy Browne, *YouTube Removes Videos Showing Atrocities in Syria*, N.Y. TIMES (Aug. 22, 2017), https://perma.cc/QT2J-F5UM; *see also* HUM. RTS. WATCH, "VIDEO UNAVAILABLE": SOCIAL MEDIA PLATFORMS REMOVE EVIDENCE OF WAR CRIMES 5-7, 22-23, 70-71 (2020), https://perma.cc/7CB5-86HT.

[41] *See, e.g.*, Lucas Schweiger, *81 of the Top 100 Public Companies Are Using Blockchain Technology*, BLOCKDATA, https://perma.cc/8MS8-DPHT (last updated Oct. 7, 2021).

[42] *See, e.g.*, Alex Hughes, Andrew Park, Jan Kietzmann & Chris Archer-Brown, *Beyond Bitcoin: What Blockchain and Distributed Ledger Technologies Mean for Firms*, 62 BUS. HORIZONS 273, 276-78 (2019).

legal and operational implications of collection methods and social media scraping,[43] these concerns are beyond the scope of this Note.

A. Defining Hashing and DLT

Hashing and DLT generally work as follows. Digital records are given a hash after collection, freezing the data and rendering it nearly impossible to alter without detection.[44] Many organizations then store records and their hashes using DLT, a storage mechanism that uses decentralized systems to protect against hackers and others who might tamper with data over long periods of time.[45] When used together, DLT and hashing have far-reaching applications in human rights advocacy and accountability efforts. Perhaps most important is the potential of these technologies to facilitate the authentication of evidence when witnesses are unavailable, allowing cases previously barred from court to proceed.[46]

1. Hashing: creating the digital fingerprint

A hash is a cryptographic tool that, once used with a piece of data like a video or an image, ensures that the data has not been altered. It can be thought of as a digital fingerprint, constructed solely from a file's contents and structure and used to verify the underlying data's authenticity.[47] A hash is created by running data through an algorithm that generates a series of numbers and letters, usually ranging between thirty-two and sixty-four characters, to replace the original data.[48] The characteristics of the resulting

[43] *See generally* DIGITAL WITNESS: USING OPEN SOURCE INFORMATION FOR HUMAN RIGHTS INVESTIGATION, DOCUMENTATION, AND ACCOUNTABILITY (Sam Dubberley, Alexa Koenig & Daragh Murray eds., 2020) (describing the opportunities and challenges surrounding open-source evidence); Nikita Mehandru & Alexa Koenig, *Open Source Evidence and the International Criminal Court*, HARV. HUM. RTS. J. (Apr. 15, 2019), https://perma.cc/KVT7-AGJ9 (discussing the increased use of open-source evidence at the ICC and the attendant opportunity for new evidentiary policies and procedures).

[44] *See* Jon Berryhill, *What Is a Hash Value?*, BERRYHILL COMPUT. FORENSICS, INC.: NEWS & COMPUT. FORENSICS BLOG (July 15, 2019), https://perma.cc/5G9B-Z27K (explaining that it would be "exceedingly complex" to replicate a hash value after altering its source data).

[45] Claudia Antal, Tudor Cioara, Ionut Anghel, Marcel Antal & Ioan Salomie, *Distributed Ledger Technology Review and Decentralized Applications Development Guidelines*, 13 FUTURE INTERNET, no. 3, Mar. 2021, at 1, 1, 10, 23.

[46] *See infra* Part III.

[47] *See* United States v. Ackerman, 831 F.3d 1292, 1294 (10th Cir. 2016) ("Some consider a hash value as a sort of digital fingerprint."); Doug Carner, Detect and Prevent File Tampering in Multimedia Files 1-2 (n.d.), https://perma.cc/B4PL-N6QN.

[48] Berryhill, *supra* note 44.

hash depend on which algorithm interacts with the input.[49] For example, applying SHA-3, a hashing algorithm, to the word "cardinal" creates the following hash:

```
adc320e142bfcd93c5e26901568b4edc4f5a59c718df3cb2ba9f
1f9723a084c699e453f9c28afd6abfb13e2dc3f56c30225ee98e
cb8745c4054db1473e2f8dc3.[50]
```

The length of a hash value does not reflect the size of the data or even what the data is, making it difficult for hackers to know exactly what a hash value corresponds to.[51]

Once the hash is created, it can be used to verify that the original data has not been tampered with or edited.[52] To verify a hash, individuals run the algorithm that was originally used to hash the data.[53] If the algorithm spits out the correct hash, the data has not been tampered with.[54] If it spits out the wrong hash, the data has been compromised in some way.[55] A key concern with hashing technology is that the algorithm will unexpectedly produce the

[49] *Cryptographic Hash Algorithms*, CODEPATH, https://perma.cc/LWN8-4D67 (archived Dec. 30, 2021).

[50] This hash was generated using the following tool: *SHA-3 Hash Generator*, CODESHACK, https://perma.cc/7SRS-RUKT (archived Dec. 30, 2021).

[51] Berryhill, *supra* note 44; Jean-Paul Delahaye, *The Mathematics of (Hacking) Passwords*, SCI. AM. (Apr. 12, 2019), https://perma.cc/86KA-SUJ6 (explaining how "the use of [digital] fingerprints can make it . . . very difficult, if not impossible, for hackers to use what they find").

[52] *See* Veronica Schmitt & Jason Jordaan, *Establishing the Validity of Md5 and Sha-1 Hashing in Digital Forensic Practice in Light of Recent Research Demonstrating Cryptographic Weaknesses in These Algorithms*, 68 INT'L J. COMPUT. APPLICATIONS, no. 23, Apr. 2013, at 40, 40-41.

[53] Berryhill, *supra* note 44 (explaining how to cross-check a hash value); *see Cryptographic Hash Algorithms*, *supra* note 49 (listing different kinds of hash algorithms).

[54] *See* Schmitt & Jordaan, *supra* note 52, at 40-42 (using quantitative study results to show that "altering even so much as one byte [of digital evidence] . . . results in a significantly different hash value"). There is an additional cryptographic tool, known as signing, that uses hashes to create and verify digital signatures. The signing process works slightly differently: The sender hashes her message and encrypts the hash with her private key. This encrypted hash becomes the "signature," which the sender includes with her message and the recipient can decrypt using the sender's public key. If the recipient's hash of the message matches the sender's decrypted hash, the recipient knows that the signed message has not been modified. *Security Tip (ST04-018): Understanding Digital Signatures*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://perma.cc/84XE-KUGF (last updated Aug. 24, 2020).

[55] Schmitt & Jordaan, *supra* note 52, at 40-42.

same hash for two different files (in what is known as a "collision"). The odds of a collision, however, are extremely low.[56]

Hashing safeguards against manipulation because *any* change to the original data—including any change to its metadata—will produce a different hash.[57] An electronic record's metadata can provide a plethora of information about that record, including the date and time of its creation, the file creator's name, and the type of device used to create it.[58] Like an MRI, the metadata illuminates the underlying physical characteristics of the record in question. Because a record's hash incorporates its metadata, comparing hashes allows individuals to ascertain whether even the metadata has been altered.[59] As a result, to manipulate data without record access, hackers would not only need to crack the hash but would also need to modify both the metadata and the original file in a way that produces a collision.[60] Though theoretically possible, in practice this is extremely unlikely.[61]

[56] Svetlin Nakov, *Crypto Hashes and Collisions*, PRAC. CRYPTOGRAPHY FOR DEVS., https://perma.cc/CXV2-FH85 (archived Dec. 30, 2021) ("Collisions in the cryptographic hash functions are extremely unlikely to be found, so crypto hashes are considered to almost uniquely identify their corresponding input." (emphasis omitted)). Even so, hashing standards will still need to evolve over time as hackers "crack" more basic hashes. *See* Roger A. Grimes, *All You Need to Know About the Move from SHA-1 to SHA-2 Encryption*, CSO (July 6, 2017, 2:45 AM PDT), https://perma.cc/B66Q-D7WD (describing the process of switching to new hash functions once industry standards can be cracked).

[57] By "original data," we mean the data on which the algorithm originally operated. Hashing can only verify the integrity of data from the point that it was hashed, not before, so timing is critical. We further develop this concern in Part III.E.1 below.

[58] *See* JENN RILEY, NAT'L INFO. STANDARDS ORG., UNDERSTANDING METADATA: WHAT IS METADATA, AND WHAT IS IT FOR? 6-7 (2017), https://perma.cc/TF4U-XJJQ; Jane Greenberg, *Understanding Metadata and Metadata Schemes*, 40 CATALOGING & CLASSIFICATION Q., nos. 3-4, 2005, at 17, 20-21.

[59] *See supra* notes 52-55 and accompanying text.

[60] *But see* ALI SUNYAEV, INTERNET COMPUTING: PRINCIPLES OF DISTRIBUTED SYSTEMS AND EMERGING INTERNET-BASED TECHNOLOGIES 277-78 (2020) (explaining how secure hashes make it hard to "reconstruct the original message"); Jesse Marks, *Distributed Ledger Technologies and Corruption: The Killer App?*, 20 COLUM. SCI. & TECH. L. REV. 42, 47-48 (2018) (noting that hash functions "cannot be reverse-engineered").

[61] United States v. Ackerman, 831 F.3d 1292, 1306 (10th Cir. 2016) (explaining that a mistaken identical hash is "unlikely if not impossible"); United States v. Miller, No. 16-cr-00047, 2017 WL 2705963, at *7 (E.D. Ky. June 23, 2017) (noting that "the digital fingerprints produced by hashing provide[d] 'virtual certainty'" that two sets of images would be identical), *aff'd*, 982 F.3d 412 (6th Cir. 2020), *cert. denied*, 141 S. Ct. 2797 (2021); *see also supra* note 60.

2. Distributed ledgers and blockchain: long-term safe storage

In its simplest form, a distributed ledger[62] is a database that preserves information in a decentralized format, distributing information across multiple locations with the involvement of multiple actors and no central control by one party.[63] This multiplicity protects against undetected hacking by facilitating transparent dialogue among many stakeholders to verify that no information has been corrupted.[64] By contrast, traditional forms of data storage rely on, and are corruptible via, a single database.[65]

Consider the following analogy: A bad actor wants to remove an incriminating photograph from a police evidence locker. While the actor could conceivably bypass the centralized owner (the officer on duty) and remove the picture, having many eyes on the photo—or copies of the photo in many different lockers—makes removal more difficult. DLT neutralizes the one-evidence-locker vulnerability for digital records. By dispersing the power of a centralized authority across a network of peers, DLT makes it difficult to alter or remove anything from the digital "locker" without detection. The absence of a hierarchy also means that this storage method lacks a single point of susceptibility.[66] The result is like a very boring, very accurate, and very public game of telephone: Each player listens in on what is being said, keeps a detailed record of how the phrase has changed, and kicks out anyone attempting to sow doubt or introduce incorrect words.

Blockchain technology is a commonly known subset of DLT and has been widely used in the financial sector. Distinguished from other forms of DLT by its use of sequencing, blockchain technology functions by absorbing a number

[62] For technical audiences, DLT should be distinguished from distributed storage systems. The former is better equipped to record iterations of data and facilitate information sharing among peers, whereas the latter offers the best solution for efficient data preservation. Rick Kuhn, Dylan Yaga & Jeffrey Voas, *Rethinking Distributed Ledger Technology*, IEEE COMPUT., Feb. 2019, at 68, 69 (explaining that a distributed ledger is a "a distributed record of transactions maintained by consensus among a network of peer-to-peer nodes"); Yin Wang & Arif Merchant, *Proportional-Share Scheduling for Distributed Storage Systems*, USENIX, https://perma.cc/CZ7R-MXE8 (last updated Jan. 3, 2007) (explaining that distributed storage systems "consolidate the separate computing and storage resources of various applications into a common pool"). We use DLT to represent both terms in this Note for simplicity.

[63] *See* Marks, *supra* note 60, at 47-55; ADVAIT DESHPANDE, KATHERINE STEWART, LOUISE LEPETIT & SALIL GUNASHEKAR, RAND EUR., UNDERSTANDING THE LANDSCAPE OF DISTRIBUTED LEDGER TECHNOLOGIES/BLOCKCHAIN: CHALLENGES, OPPORTUNITIES, AND THE PROSPECTS FOR STANDARDS, at ix (2017), https://perma.cc/ZCX3-RHM8.

[64] *See* DESHPANDE ET AL., *supra* note 63, at 1-2.

[65] *See* SUNYAEV, *supra* note 60, at 266-67.

[66] *See* Marks, *supra* note 60, at 48 (explaining how distributed-ledger "nodes" reject changes that are inconsistent with their own calculations and with the network consensus).

of transactions or data points, collating them into a block, and then linking the block to a larger chain.[67] The broader category of distributed ledgers does not require such a structure.

Much of the popular discourse around consensus-driven models has focused on the rise of cryptocurrency, but the potential applications of DLT extend far beyond that realm and include digital evidence preservation in the context of human rights.[68] Specifically, distributed ledgers: (1) allow human rights organizations to safeguard raw evidence of abuses; and (2) facilitate collaboration with other experts in the field.[69] These tasks can be accomplished using both public and private ledgers.[70] The former type of platform acts as a consensus service for the public at large: Public distributed-ledger networks allow anyone to view the ledger, validate data, and upload additional information, all without impacting the preexisting data package.[71] These networks function independently from private distributed ledgers, where only specific individuals (here, human rights organizations and their partners) can upload information and replicate the data package.[72] This distinction is more than a mere public and semiprivate divide. Public ledgers promote integrity and transparency with external actors, while private ledgers allow human rights organizations to safeguard proprietary information, record assertions of veracity from experts, and build improvements into, for example, event-prediction technology.[73]

[67] *See* SUNYAEV, *supra* note 60, at 275.

[68] *See* William Thomas Weilbach & Yusuf Moosa Motara, *Applying Distributed Ledger Technology to Digital Evidence Integrity*, 110 SAIEE AFR. RSCH. J. 77, 77 (2019). For one example of a distributed-ledger framework focused on human rights, see STARLING LAB, https://perma.cc/6D8Z-VKLB (archived Dec. 30, 2021) ("Starling is innovating with the latest cryptographic methods and decentralized web protocols to meet the technical and ethical challenges of establishing trust in our most sensitive digital records, such as the documentation of human rights violations, war crimes and testimony of genocide.").

[69] *See* WITNESS, TICKS OR IT DIDN'T HAPPEN: CONFRONTING KEY DILEMMAS IN AUTHENTICITY INFRASTRUCTURE FOR MULTIMEDIA 4, 34-36 (2019), https://perma.cc/7U78-JH2N.

[70] *See* SUNYAEV, *supra* note 60, at 276.

[71] *Id.*

[72] *Id.* The fact that any node within the network can view data and related transactions on the ledger enables circulation of evidence among credible peer entities.

[73] *Cf.* Antal et al., *supra* note 45, at 10 (explaining the trade-offs between public and private ledgers in the corporate context).

B. Hashing and DLT in Human Rights Litigation

As human rights organizations and documenters adapt to changing technological capabilities, the use of hashing and DLT has begun to take root.[74] Leading human rights groups are discussing these technologies as applied to their work,[75] and best practices have already begun to crystallize around the incorporation of DLT and hashing.[76] While many citizens still rely on personal hard drives or hosting sites like YouTube to preserve data, hashing evidence and storing it using DLT has become an increasingly popular practice among sophisticated evidence-collection organizations.[77]

Used together, hashing and DLT help establish a chain of custody by forming a self-reinforcing barrier against data corruption.[78] First, hashing facilitates safe transmission between devices (for example, between a phone and a computer server) by ensuring that data is not manipulated while being transmitted or stored.[79] Since courts are often concerned with potential manipulation during the temporal gap between the collection of data and its submission as evidence,[80] hashing at the moment of capture certifies that nothing improper has occurred during the intervening period. Second, DLT places the hashed data into a secure network for extended storage. This

[74] *See, e.g.*, WITNESS, *supra* note 69, at 4, 58; Beth Van Schaack, *The Fourth Industrial Revolution Comes to The Hague*, ICC F., https://perma.cc/T7UD-XWPQ (archived Dec. 30, 2021).

[75] *See, e.g.*, HUM. RTS. WATCH, SPARKLING JEWELS, OPAQUE SUPPLY CHAINS: JEWELRY COMPANIES, CHANGING SOURCING PRACTICES, AND COVID-19 39-40 (2020), https://perma.cc/8ZUN-QRCK (examining the use of blockchain technology to enhance the traceability of ethically sourced jewelry). *See generally* ARTICLE 19, BLOCKCHAIN AND FREEDOM OF EXPRESSION (2019), https://perma.cc/YB5V-TCHQ (examining the promises and potential shortcomings of blockchain technology with respect to advancing freedom of expression).

[76] *See, e.g.*, *Using Metadata to Prove the Reliability and Validity of Footage*, EYEWITNESS, https://perma.cc/ER4Z-KQNC (archived Dec. 30, 2021) (explaining how one leading model for human rights documentation relies on hashing and "unique" metadata collection and storage); *How DLT Is Fighting the Information War in Syria and Saving Lives*, FORKAST (Jan. 5, 2021, 4:02 PM HKT), https://perma.cc/255H-RLM9 (discussing how DLT can prevent civilian casualties and boost confidence in data).

[77] *See* WITNESS, *supra* note 69, at 58 ("Many of the companies interviewed for this report are using blockchain technologies as a way of tracking the chain of custody of digital evidence, and providing a decentralized and public way to track the provenance and authenticity of an image, video or audio recording.").

[78] *See infra* Part III.C.1.

[79] *See supra* Part II.A.1.

[80] *See infra* Part III.C.1.

process—from the point of upload to the distribution across ledgers—can take place almost instantaneously, with little to no human intervention.[81]

Once evidence has been hashed and distributed, it is virtually impervious to manipulation.[82] Just as critically, all evidence that is collected and stored using this method remains secure for long-term preservation, because this process repeats in a continuously decentralized fashion.[83] These features combine to help facilitate evidence authentication. Additional benefits to hashing and DLT include increased safety surrounding the collection of evidence and the elimination of the "YouTube problem," where video evidence of human rights abuses uploaded to YouTube or other online platforms is taken down.[84] Rather than storing evidence on a single hard drive or in personal cloud storage, an individual can upload files to a secure digital location with multiple custodians, minimizing risks to the life of the individual and the integrity of the files.[85]

The work of Muhammad Najem provides an excellent example of how hashing and DLT can be used in the human rights context. Najem, a fifteen-year-old Syrian national, leveraged these technologies to preserve his ad hoc documentation of airstrikes in Ghouta, Syria.[86] Najem's "selfie videos" aimed to document the devastation that befell his neighborhood, and they ultimately became part of a journalistic effort to attract the attention of world leaders who had failed to intervene in the Syrian conflict.[87] At first, Najem's videos were met with skepticism, including accusations that he was lying about his location.[88] In response, Najem began using a service called Truepic to inscribe

[81] *See* DESHPANDE ET AL., *supra* note 63, at xi tbl.1 (listing the automation of DLT solutions as one of the "[k]ey . . . opportunities in relation to DLT/blockchain").

[82] SUNYAEV, *supra* note 60, at 266 ("By applying cryptographic techniques, transactions, and represented assets are safeguarded from manipulation and theft.").

[83] *See* WORLD BANK GRP., DISTRIBUTED LEDGER TECHNOLOGY (DLT) AND BLOCKCHAIN 16 (2017), https://perma.cc/2NQU-EFYU (discussing the "[e]nhanced cybersecurity resilience" afforded by DLT); Weilbach & Motara, *supra* note 68, at 80 ("The transparency and immutability of the blockchain can ensure that the evidence is preserved for as long as the blockchain itself exists . . . .").

[84] HUM. RTS. WATCH, *supra* note 40, at 6-12 (noting the opaque practices around the removal of sensitive material); *see also* Billy Perrigo, *These Tech Companies Managed to Eradicate ISIS Content. But They're Also Erasing Crucial Evidence of War Crimes*, TIME (Apr. 11, 2020, 8:00 AM EDT), https://perma.cc/FT5C-3AHY (describing how broad content-moderation policies have led to the removal of "innocent photos and videos, especially from war zones").

[85] *See supra* note 39 and accompanying text.

[86] Nora Neus, *The 15-Year-Old Documenting Eastern Ghouta Massacre with Selfie Videos*, CNN (Feb. 21, 2018, 8:11 AM EST), https://perma.cc/J2X3-HGAX; WITNESS, *supra* note 69, at 22.

[87] *See* Neus, *supra* note 86.

[88] WITNESS, *supra* note 69, at 22.

his videos with immutable metadata, hash the videos, and store them on a blockchain connected to the company's servers.[89] With the additional verification provided by Truepic, at least one of Najem's videos was "trusted and disseminated by mainstream media networks" around the world.[90] Amid the rise of deepfakes and other data-manipulation tools, hashing and DLT gave Najem a way to verify his videos and validate his lived experience. These technologies can also take evidence a step further, allowing someone like Najem to authenticate his videos in a court of law.

III. Authenticating Digital Evidence Stored Using Hashing and DLT Without Witnesses

The U.S. legal system has historically relied on witnesses to authenticate both physical and digital evidence. For example, investigators may (and sometimes must) testify to the authenticity of certain physical evidence recovered from a crime scene.[91] But this reliance on witness testimony creates issues in human rights litigation, especially when a case is predicated on evidence collected by civilians or journalists.[92] Using live witness testimony in certain human rights cases, like those regarding war crimes, can be especially dangerous. Revealing a documenter's identity may put that individual's safety at risk.[93]

As the Muhammad Najem example demonstrates, hashing and DLT can both provide safe, long-term digital evidence storage and validate photos and

[89] *Id.*; *Our Technology*, TRUEPIC, https://perma.cc/P4BZ-L8DN (archived Dec. 30, 2021).

[90] WITNESS, *supra* note 69, at 22.

[91] FED. R. EVID. 901; *see, e.g.*, United States v. Collado, 957 F.2d 38, 39-40 (1st Cir. 1992) (holding that evidence was properly authenticated when a police officer testified that it was the same evidence he had seized at the scene).

[92] Though witness participation often plays a central role in human rights and international criminal litigation, the International Military Tribunal at Nuremberg was a notable exception. *See* Freeman, *supra* note 23, at 299 (noting that the decision to rely primarily on documentary evidence was "against common wisdom").

[93] This problem can be particularly acute in conflict settings, cases involving abuses committed by internal security forces, and cases that require testimony from members of vulnerable groups. *See, e.g.*, Patricia M. Wald, Note from the Field, *Dealing with Witnesses in War Crime Trials: Lessons from the Yugoslav Tribunal*, 5 YALE HUM. RTS. & DEV. L.J. 217, 220 (2002) (discussing the "perpetual state of fear of retaliation" that victims and prospective witnesses experience); James v. Donovan, 14 N.Y.S.3d 435, 438-39, 441 (App. Div. 2015) (noting the importance of secret witness testimony in a high-profile police-abuse case); *Protecting Witnesses and Victims: Special Measures for Women and Children*, OFF. U.N. HIGH COMM'R FOR HUM. RTS. (July 29, 2011), https://perma.cc/CJG4-8Z25 (highlighting the unique risks that testifying can pose for certain women and children).

videos in the public media sphere.[94] But these technologies also have the potential to transform evidence in the courtroom, possibly alleviating the need for witness testimony regarding authentication. This development is attractive for two reasons. First, it saves money by eliminating the need for legal teams to obtain witnesses every time they present evidence. Second, it narrows the evidentiary gap left when witnesses are unavailable or unwilling to testify, a problem that is particularly common in international human rights and criminal cases.[95] This Part queries whether and how hashing and DLT can facilitate authentication in U.S. evidence law. We do not intend to assert that human rights litigation can or should abandon the use of witness testimony altogether.[96] Rather, our goal is to illuminate avenues for justice when obtaining witness testimony is impracticable due to exigent factors. The potential drawbacks of authentication without witness testimony are addressed in Part III.E below.

A. General Evidentiary Requirements for Authentication

As a threshold matter, evidence admitted in U.S. courts must be relevant to a material issue and properly authenticated.[97] Under Rule 901(a) of the Federal Rules of Evidence, an item must be authenticated by additional evidence "sufficient to support a finding that the item is what the proponent claims it is."[98] In other words, authentication is achieved by showing that a piece of evidence is "an accurate depiction of a particular person, place, object, or event."[99] Beyond the intuitive desire to keep falsified evidence out of the courtroom, authentication is important because the Anglo-American system generally prefers evidence that is presented under oath, directly observable by the jury, and subject to cross-examination.[100] For photographic or video

[94] *See supra* notes 86-90 and accompanying text.

[95] *See* INT'L COUNCIL ON HUM. RTS. POL'Y, HARD CASES: BRINGING HUMAN RIGHTS VIOLATORS TO JUSTICE ABROAD 43-44 (1999), https://perma.cc/J8D8-CXWB.

[96] In fact, there are some areas where witness testimony can be critical, such as determining the proper weight to afford a piece of evidence once it is admitted. *See, e.g.*, Turner v. Knight Transp., Inc., No. 13-cv-02864, 2016 WL 1259891, at *1 (W.D. La. Mar. 28, 2016) (noting that witness testimony can help the jury decide "the evidence's true authenticity and probative value").

[97] FED. R. EVID. 401, 901(a). Authentication constitutes only one part of the admissibility determination and does not cure other evidentiary issues. For example, a piece of evidence could be authenticated under Rule 901 but still be excludable due to unfair prejudice or hearsay considerations. *See id.* R. 403, 802.

[98] *Id.* R. 901(a).

[99] State v. Haight-Gyuro, 186 P.3d 33, 35 (Ariz. Ct. App. 2008).

[100] *See* GLEN WEISSENBERGER & JAMES J. DUANE, WEISSENBERGER'S FEDERAL EVIDENCE § 801.1, at 502-03 (7th ed. 2011) ("The common law of evidence developed a system of exclusion that rejects the admission of much evidence that fails to satisfy these three

footnote continued on next page

evidence, authentication "frequently takes the form of witness testimony that the photograph or video accurately portrays whatever it purportedly depicts."[101] A witness is not always required, however, to authenticate a photo or video. Indeed, Rule 901(b) provides a nonexhaustive list of evidence that can be submitted in lieu of witness testimony, including evidence outlining distinctive characteristics of the proffered item,[102] evidence regarding public records,[103] and evidence showing that a particular process or system produces an accurate result.[104]

This nonexhaustive list not only provides a roadmap for litigants to authenticate evidence, but also allows judges to use their discretion in deciding what evidence is sufficient to authenticate a photo or video for the purposes of Rule 901.[105] Courts have explicitly recognized that decisions regarding authentication "rest[] within the sound discretion of the trial judge."[106] This discretion is protected on appeal, where a trial judge's determination of admissibility (and therefore authenticity) can be overturned only on a showing of "clear abuse of discretion."[107] This standard sets a high bar for challenging the admission of evidence, and thus grants significant power to trial judges in determining what can and cannot serve as evidence in a given case. In light of this trial-court discretion, it is critical to analyze how evidence stored using DLT and hashing might map onto existing evidentiary standards so that judges and litigants alike can make informed judgments on admissibility.

Unsurprisingly, judicial discretion produces inconsistent authentication analyses. Some courts apply a minimal standard of authentication for admitting evidence, while others require a preponderance of the evidence to establish authenticity.[108] Still others interpret authenticity to mean whether a

safeguards."). In fact, the Sixth Amendment often demands live testimony in criminal cases. *See* Ohio v. Clark, 135 S. Ct. 2173, 2179-81 (2015) (discussing recent precedent regarding the Confrontation Clause).

[101] *Haight-Gyuro*, 186 P.3d at 35.

[102] FED. R. EVID. 901(b)(4).

[103] *Id.* R. 901(b)(7).

[104] *Id.* R. 901(b)(9). In the human rights context, this could involve evidence that a particular capture or storage system produces a photo or video without manipulation.

[105] *Cf.* United States v. Cejas, 761 F.3d 717, 725 (7th Cir. 2014) (holding that the district court did not abuse its discretion in admitting video evidence that it determined to be sufficiently authenticated by witness testimony).

[106] United States v. Rembert, 863 F.2d 1023, 1027 (D.C. Cir. 1988) (quoting United States v. Blackwell, 694 F.2d 1325, 1330 (D.C. Cir. 1982)).

[107] *Id.* (quoting *Blackwell*, 694 F.2d at 1330).

[108] *Compare* United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007) (requiring only a minimal standard for authentication), *and* McQueeney v. Wilmington Tr. Co., 779 F.2d 916, 928 (3d Cir. 1985) ("The burden of proof for authentication is slight."), *with* United States v. Grant, 967 F.2d 81, 82 (2d Cir. 1992) (per curiam) ("Federal Rule of Evidence 901

footnote continued on next page

reasonable juror could find the evidence authentic.[109] That said, most courts do not require litigants to rule out "all possibilities inconsistent with authenticity," nor do they require proof "beyond any doubt."[110] In other words, "[o]nly a prima facie showing of genuineness is required," and the appropriate weight of the evidence rests in the hands of the jury.[111] Additionally, the Federal Rules of Evidence allow for some forms of evidence to be self-authenticating, meaning that these forms require no additional evidence to establish their authenticity.[112] We now turn to these rules and their applicability to digital evidence stored using hashing and DLT.

B. Hashing and DLT as Self-Authenticating

We start with self-authentication, perhaps the most straightforward and textually supported method for admitting evidence without witness testimony. As noted above, self-authentication allows evidence to be admitted without "extrinsic evidence of authenticity."[113] Rule 902 lists the narrow categories of evidence that qualify as self-authenticating.[114] Relevant for our analysis is Rule 902(14)'s allowance of "certified data copied from an electronic device, storage medium, or file."[115] As long as the evidence is "authenticated by a process of digital identification, as shown by a certification of a qualified person,"[116] Rule 902(14) dispenses with the need for live testimony. Although the certification requirement is somewhat vague, the Rules permit "a qualified person [to certify] that she checked the hash value of the proffered item and that it was identical to the original."[117] While "qualified person" is not defined, such an individual could conceivably be an engineer or an operator of the

requires . . . a showing, by a preponderance of evidence, that the thing offered is what its proponent claims it to be.").

[109] *See Rembert*, 863 F.2d at 1027; Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 8 & n.22 (2009).

[110] State v. Ruggiero, 35 A.3d 616, 622 (N.H. 2011) (quoting *Gagliardi*, 506 F.3d at 151); *see also* United States v. Barlow, 568 F.3d 215, 220 (5th Cir. 2009) (noting that the standard for authentication is not "burdensome").

[111] United States v. Fluker, 698 F.3d 988, 999 (7th Cir. 2012); *see also* Turner v. Knight Transp., Inc., No. 13-cv-02864, 2016 WL 1259891, at *1 (W.D. La. Mar. 28, 2016).

[112] FED. R. EVID. 902.

[113] *Id. But see* Goode, *supra* note 109, at 9 n.25 (noting that some forms of self-authenticating evidence must still be accompanied by a written declaration).

[114] *See* FED. R. EVID. 902.

[115] *Id.* R. 902(14) (capitalization altered).

[116] *Id.*

[117] *Id.* R. 902(14) advisory committee's note to 2017 amendment.

relevant system.[118] The Supreme Court has never weighed in on the constitutional contours of Rule 902(14), and case law is still nascent in this area.[119] Accordingly, our analysis is largely theoretical and focuses on the general application of Rule 902(14).[120]

While there is little jurisprudence on Rule 902(14), the discussion above suggests that prosecutors can use the rule to authenticate digital evidence, especially evidence that is hashed. Indeed, the Advisory Committee specifically imagined processes generating hash values as falling under Rule 902(14).[121] DLT could also fall within the ambit of Rule 902(14) because the ledger, by continuously guarding against hash alterations over a long period of time, provides a process of digital identification.

But Rule 902(14) also places additional burdens on litigants seeking to self-authenticate evidence. For domestic records, the rule stipulates that the certification must meet the requirements outlined in Rule 902(11).[122] Two of these requirements are easily surmountable: (1) "a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court"; and (2) pretrial "reasonable written notice of the intent to offer the record."[123] The first three requirements of Rule 803(6), which the certification must also satisfy per Rule 902(11), are more challenging:

[118] Courts could also look to forensic analysts or e-discovery experts to make these certifications. *See* Ramona L. Lampley, *Something Old and Something New: Exploring the Recent Amendments to the Federal Rules of Evidence*, 57 WASHBURN L.J. 519, 524 (2018).

[119] *See id.* at 519 (noting the recent adoption of Rule 902(14)); John Patzakis, *Rule of Evidence 902(13)(14) Update: States Begin Adoption, First Case Citations*, X1: NEXT GEN GRC & EDISCOVERY L. BLOG (Mar. 19, 2019), https://perma.cc/KJD5-SYYW.

[120] Authentication exists separate and apart from other admissibility standards: The commentary to Rule 902(14) specifies that the provision does not circumvent other evidentiary rules like "hearsay, relevance, or in criminal cases the right to confrontation." FED. R. EVID. 902(14) advisory committee's note to 2017 amendment. For example, a distributed ledger could preserve and prove the authenticity of an audio recording, but the recording's contents would still have to fall under a hearsay exception (or not be hearsay) to be admitted into evidence. *See id.* R. 801, 803. In other words, although DLT and hashing may address authenticity issues, litigants seeking to leverage these technologies should keep in mind other evidentiary rules.

[121] *See supra* note 117 and accompanying text. The commentary to Rule 902(14) also mentions that certification can take place "through processes other than comparison of hash value, including by other reliable means of identification provided by future technology." FED. R. EVID. 902(14) advisory committee's note to 2017 amendment.

[122] FED. R. EVID. 902(14). For records stored outside the United States, the certification must comply with local law rather than a federal statute or Supreme Court rule. *Id.* R. 902(12); *see infra* note 123 and accompanying text. Otherwise, the requirements are the same for these records and for domestic records. *See* FED. R. EVID. 902(12).

[123] FED. R. EVID. 902(11).

> (A) the record was made at or near the time by—or from information transmitted by—someone with knowledge;
>
> (B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit; [and]
>
> (C) making the record was a *regular* practice of that activity . . . .[124]

In the human rights space, many journalists and civilians who document abuses simply happen to be on the scene when the abuse occurs.[125] A court might view the inherently erratic nature of this kind of documentation as far from "regular," thus imperiling the self-authentication analysis.

Furthermore, the Advisory Committee's comments to Rule 803(b)(6) indicate that the rule exists because business records are unusually reliable: Businesses have an incentive to systematically check and verify their files.[126] Absent a centralized human rights organization that maintains a distributed ledger and handles hashing,[127] the prospect of admitting evidence provided by a journalist or a citizen under Rule 902(14) may thus be slim. The requirements embedded in the rule raise significant barriers to self-authentication without an organization that regularly stores evidence of human rights abuses.

C. Other Doctrines for Authenticating Digital Evidence Without Witnesses

Should self-authentication fail, common law doctrines may still allow for the admission of evidence protected via hashing and DLT without witness testimony. We discuss four of these doctrines below: (1) chain of custody; (2) the silent-witness theory; (3) distinctive characteristics; and (4) the reply-letter doctrine.

[124] *Id.* R. 803(6) (emphasis added); *see id.* R. 902(11) (stating that records must meet these three requirements).

[125] *See* David Batty, *Arab Spring Leads Surge in Events Captured on Cameraphones*, GUARDIAN (Dec. 29, 2011, 2:23 PM EST), https://perma.cc/3ES3-8VZF ("In most cases citizens capture the breaking news moments first." (quoting Al Jazeera employee Riyaad Minty)).

[126] *See* FED. R. EVID. 803(6) advisory committee's note to 1972 proposed rules ("The element of unusual reliability of business records is said variously to be supplied by systematic checking, by regularity and continuity which produce habits of precision, by actual experience of business in relying upon them, or by a duty to make an accurate record as part of a continuing job or occupation.").

[127] A centralized private ledger for human rights documentation is likely the most effective way to ensure the self-authentication of digital content under the Federal Rules of Evidence. *See infra* Part III.D.

1. Chain of custody

U.S. courts typically recognize that establishing a "chain of custody" is sufficient to meet the requirements of Rule 901.[128] This well-known common law doctrine, traditionally applied to physical objects, traces the path that a piece of evidence takes from the moment it becomes legally relevant to the moment it is presented in court, in order to establish that it has not been altered.[129] A quintessential example of the chain-of-custody doctrine involves a piece of hair that is found at a crime scene. To introduce the strand of hair into evidence, a prosecutor could show that a forensic investigator found it at the crime scene and transferred it to an evidence locker where it remained untouched until the moment of trial. The prosecutor would have to account for additional links in the chain if the strand of hair entered anyone else's custody (such as a forensic analyst's) between its collection and its presentation at trial.[130] Courts differ in terms of what evidence they require to verify the chain of custody. While courts have commonly used nontestimonial evidence to establish a chain,[131] the Constitution may now demand live testimony in certain chain-of-custody instances.[132]

A chain of custody need not be perfect for a piece of evidence to be admissible.[133] Instead, the ultimate question is whether the chain of custody is "sufficiently complete so as to convince the court that it is improbable that the original item had been exchanged with another or otherwise tampered with."[134] Once admitted, any gaps in the chain of custody "go to the weight of the evidence."[135]

[128] *See* Paul C. Giannelli, *Chain of Custody and the Identification of Real Evidence*, 6 PUB. DEF. REP., no. 2, Mar.-Apr. 1983, at 1, 1.

[129] *See id.* at 1, 3-4 (summarizing the chain-of-custody doctrine).

[130] *Id.* at 4.

[131] *See* United States v. Jones, 356 F.3d 529, 536 (4th Cir. 2004) (upholding the admission of evidence based on a chain of custody established in part by a shipping form).

[132] *See* Melendez-Diaz v. Massachusetts, 557 U.S. 305, 311 n.1 (2009) ("It is up to the prosecution to decide what steps in the chain of custody are so crucial as to require evidence; but what testimony *is* introduced must . . . be introduced live."). *But cf. id.* ("[D]ocuments prepared in the regular course of equipment maintenance may well qualify as nontestimonial records."); United States v. Johnson, 688 F.3d 494, 505 (8th Cir. 2012) ("[C]hain of custody alone does not implicate the Confrontation Clause.").

[133] United States v. Thomas, 749 F.3d 1302, 1310 (10th Cir. 2014).

[134] United States v. Grant, 967 F.2d 81, 83 (2d Cir. 1992) (per curiam) (quoting United States v. Howard-Arias, 679 F.2d 363, 366 (4th Cir. 1982)).

[135] United States v. Tatum, 548 F.3d 584, 587 (7th Cir. 2008) (quoting United States v. Scott, 19 F.3d 1238, 1245 (7th Cir. 1994)).

Significant gaps in the chain of custody, however, may be serious enough to require exclusion.[136] To assess an allegedly faulty chain, courts look for "ample corroborative evidence as to [the evidence's] acquisition and subsequent custody."[137] For digital evidence, courts would similarly require an adequate record of the data's life cycle: its collection, storage, analysis, and presentation. Such life cycles have been used to authenticate evidence from surveillance cameras in situations where no witnesses could testify to an event's occurrence.[138] Indeed, courts have admitted surveillance videos when supplemented with evidence regarding the chain of custody and film development.[139] Similar logic applies to cases involving photographs.[140]

By establishing a clear chain of custody, DLT can enable the introduction of digital evidence in the absence of direct witness testimony. Without DLT, photos and videos of human rights abuses are often uploaded to public forums like YouTube, potentially disrupting the chain of custody. Of course, YouTube can remove videos entirely.[141] But even absent removal, platforms like YouTube present a significant vulnerability. A conventional chain of custody involves testimony from each person who had possession of an object concerning (1) the duration of their custody; (2) precautions they took to safeguard the object; (3) evidence that the object was not tampered with; and (4) evidence of the object's timely transfer to the next custodian.[142] When digital evidence is placed on public platforms, it is not always possible to hale everyone who had access to the data into court.

DLT addresses chain-of-custody problems by decentralizing the storage process. There is no central custodian in a blockchain-based evidence ledger;[143] no individual has the power to enter the "digital evidence locker" and alter its

[136] *See, e.g.*, United States v. Bonds, No. 07-cr-00732, 2009 WL 416445, at *1-2 (N.D. Cal. Feb. 19, 2009), *aff'd*, 608 F.3d 495 (9th Cir. 2010).

[137] United States v. Mitchell, 816 F.3d 865, 872 (D.C. Cir. 2016) (alteration in original) (quoting United States v. Mejia, 597 F.3d 1329, 1336 (D.C. Cir. 2010)).

[138] *See, e.g.*, United States v. Pageau, 526 F. Supp. 1221, 1224 (N.D.N.Y. 1981).

[139] *See id.*; State v. Young, 303 A.2d 113, 116 (Me. 1973).

[140] *See* United States v. Taylor, 530 F.2d 639, 641-42 (5th Cir. 1976); Litton v. Commonwealth, 597 S.W.2d 616, 619-20 (Ky. 1980); State v. Pulphus, 465 A.2d 153, 161 (R.I. 1983).

[141] *See supra* note 40 and accompanying text.

[142] *See, e.g.*, United States v. Thomas, 749 F.3d 1302, 1310-11 (10th Cir. 2014) (using a nine-step chain of custody to authenticate drug evidence where an officer testified to the receipt, storage, transfer for analysis, and return of the drugs to storage).

[143] *See* Angela Guo, *Blockchain Receipts: Patentability and Admissibility in Court*, 16 CHI.-KENT J. INTELL. PROP. 440, 441 (2017) (describing the general operation of a blockchain ledger); *supra* notes 62-64 and accompanying text. That said, there must still be a host to oversee the functioning of the distributed ledger. We partially address this issue in Part IV.B below.

contents.[144] DLT can therefore establish a chain of custody without requiring witnesses to come to court. Because the technology keeps an immutable record of all interactions with the underlying data,[145] prosecutors do not need to interrogate everyone with data access (like software engineers) to ensure that the chain of custody is sound. Instead, the ledger itself prevents individuals from inappropriately accessing or altering the data.[146] Additionally, hashing can verify that the data has not changed since its initial hash (and possibly its initial capture), even if it was stored years ago.[147] Together, hashing and DLT work to accomplish the twin goals of the chain-of-custody doctrine: establishing the original identity of an object and verifying that it was not manipulated along the way.

2. Silent-witness theory

The silent-witness theory allows parties to forgo the witness-testimony requirement if they establish the integrity of the process that produced the evidence.[148] This doctrine was first used to admit X-rays, and courts now rely on it to authenticate footage from automatic cameras and surveillance systems.[149] While nearly all jurisdictions allow authentication using the silent-witness theory,[150] courts hold differing views about which evidentiary standards must be met. Some jurisdictions use a multi-factor approach to evaluate authenticity, taking into account evidence related to operator competency, the likelihood that alterations or tampering occurred, the manner

[144] *Cf.* Guo, *supra* note 143, at 441 (explaining that "no sole organization" can disrupt the accounts of digital currency users).

[145] *See supra* Part II.A.2.

[146] *See* Guo, *supra* note 143, at 443. Although Guo notes that an individual could "alter the master sheet" by controlling "a dispositive majority" of the network, such a feat is "virtually impossible" with a large number of users. *Id.*

[147] *See supra* Part II.A.1.

[148] 16 AM. JUR. 3D *Proof of Facts* § 5 (West 2022); People v. Taylor, 956 N.E.2d 431, 438 (Ill. 2011).

[149] *See* 16 AM. JUR. 3D *Proof of Facts* § 5; Tracy Bateman Farrell, Annotation, *Construction and Application of Silent Witness Theory*, 116 A.L.R. 5th 373, § 2[a] (2004); *see also* 16 AM. JUR. 3D *Proof of Facts* § 25 ("Automatic surveillance pictures are, of course, one of the prototypical situations in which the 'silent witness' theory has been applied.").

[150] *See* JOHN W. STRONG, KENNETH S. BROUN, GEORGE E. DIX, EDWARD J. IMWINKELRIED, D.H. KAYE, ROBERT P. MOSTELLER & E.F. ROBERTS, MCCORMICK ON EVIDENCE § 214, at 343 (5th ed. 1999). *See generally* Diane M. Allen, Annotation, *Admissibility of Visual Recording of Event or Matter Giving Rise to Litigation or Prosecution*, 41 A.L.R. 4th 812 (1985) (citing federal and state cases admitting evidence under the silent-witness theory). The silent-witness theory has also been adopted by several military courts. United States v. Harris, 55 M.J. 433, 438 (C.A.A.F. 2001); United States v. Howell, 16 M.J. 1003, 1005-06 (A.C.M.R. 1983); United States v. Reichart, 31 M.J. 521, 523-24 (A.C.M.R. 1990) (per curiam).

in which the evidence was preserved, the speakers or persons pictured, the date or time of the evidentiary capture, and the reliability of the system.[151] All of these factors illuminate whether the system was "capable of recording what a witness would have seen or heard had a witness been present at the scene."[152] Other jurisdictions use a flexible, fact-specific approach, allowing room for secondary evidence that may "bear[] on whether the . . . [main] evidence correctly depicts what it purports to represent."[153] Although witness testimony has often been used to establish the soundness of capture and storage mechanisms under the silent-witness theory, at least some courts have recognized that witness testimony is not always required to establish reliability.[154]

Regardless of the analytical approach adopted, the silent-witness analysis focuses on whether evidence was captured and stored in a sound manner.[155] Some courts have noted that this analysis is only appropriate when there are no witnesses to an event.[156] This constraint is not universal, however, as other courts have determined that the silent-witness theory is appropriate when no

[151] *See Ex parte* Fuller, 620 So. 2d 675, 678 (Ala. 1993) (applying a seven-factor analysis); Wagner v. State, 707 So. 2d 827, 831 (Fla. Dist. Ct. App. 1998) (applying a five-factor analysis).

[152] *Fuller*, 620 So. 2d at 678.

[153] State v. Anglemyer, 691 N.W.2d 153, 162 (Neb. 2005); *see* United States v. Reed, 887 F.2d 1398, 1405 (11th Cir. 1989) (holding that "the trial court has broad discretion to allow [cassette] tapes into evidence without [a factor-based] showing so long as there is independent evidence of accuracy"); Fisher v. State, 643 S.W.2d 571, 575 (Ark. Ct. App. 1982) ("It is neither possible nor wise to establish specific foundational requirements for the admissibility of . . . evidence under the 'silent witness' theory . . . ."); Dep't of Pub. Safety & Corr. Servs. v. Cole, 672 A.2d 1115, 1122 (Md. 1996) ("We decline to adopt any rigid, fixed foundational requirements necessary to authenticate . . . evidence under the 'silent witness' theory."); State v. Haight-Gyuro, 186 P.3d 33, 37 (Ariz. Ct. App. 2008) (adopting a "flexible approach" that allows trial courts "to consider the unique facts and circumstances in each case").

[154] *See, e.g.*, People v. Taylor, 956 N.E.2d 431, 441, 443 (Ill. 2011) (finding that a videotape was admissible based in part on a written police report); *Harris*, 55 M.J. at 439 ("The reliability of [a] camera system can, but need not, be shown by an expert witness."); *see also* United States v. Fadayini, 28 F.3d 1236, 1241 (D.C. Cir. 1994) (concluding that photos taken at an ATM were sufficiently authenticated by the indirect testimony of bank personnel); State v. Colby, 431 A.2d 462, 464 (Vt. 1981) (concluding that surveillance photographs were properly admitted based on evidence of their accuracy and indirect testimony).

[155] *See* United States v. Taylor, 530 F.2d 639, 641-42 (5th Cir. 1976) (allowing the admission of photographs based on testimony regarding "the manner in which the film was installed in the camera, how the camera was activated, the fact that the film was removed immediately after the robbery, the chain of its possession, and the fact that it was properly developed and contact prints made from it").

[156] *See, e.g.*, State v. Stangle, 97 A.3d 634, 637 (N.H. 2014) (stating that the silent-witness theory is appropriate when there are no firsthand witnesses).

witness "can" testify.[157] In any event, a lack of available witnesses can be overcome without relying on the silent-witness theory by providing evidence regarding the process of collection and storage under Rule 901(b)(9).[158]

The silent-witness theory works well with hashing and DLT because these technologies guarantee security of process. Hashing creates a digital fingerprint for data, allowing individuals to detect unwanted alteration. Similarly, DLT protects data from manipulation.[159] Thus, in the same way that courts have recognized authenticity when an "asset protection manager" testifies to the capture, storage, and transfer processes for surveillance cameras,[160] DLT and hashing can establish reliability without requiring testimony from individuals who directly witnessed an event. Because hashing and DLT protect against mutability, litigants will have little difficulty proving authenticity when alterations or irregularities are alleged, even when a case takes place long after abuses have occurred.[161]

3. Distinctive-characteristics doctrine

The distinctive-characteristics doctrine is "one of the most frequently used [methods] to authenticate e-mail and other electronic records."[162] The doctrine, embodied in Rule 901(b)(4), states that evidence can be authenticated when the "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances," indicate that the proffered evidence is what the proponent claims it to be.[163] The commentary to Rule 901(b)(4) indicates that a wide variety of specific characteristics can be used for authentication, including language patterns and

[157] *Ex parte* Rieber, 663 So. 2d 999, 1008-09 (Ala. 1995) (analyzing a videotape under the silent-witness theory where no witness could testify as to what appeared in the tape footage); *see also* Cheng & Nunn, *supra* note 13, at 1120 (proposing a regime that contemplates greater reliance on the silent-witness theory).

[158] Under Rule 901(b)(9), evidence can be authenticated by "describing a process or system and showing that it produces an accurate result." FED. R. EVID. 901(b)(9). X-rays are commonly admitted under this rule, as are videos from surveillance cameras. *See id.* R. 901(b)(9) advisory committee's note to 1972 proposed rules; State v. Snead, 783 S.E.2d 733, 736 (N.C. 2016).

[159] *See supra* Part II.A.

[160] *See Stangle*, 97 A.3d at 639.

[161] This is a common phenomenon in human rights litigation. *See, e.g.*, Kreshnik Gashi & Xhorxhina Bami, *Kosovo Special Prosecutor: "Wartime Rape Victims Must Speak Out,"* BALKAN INSIGHT: BALKAN TRANSITIONAL JUST. (July 8, 2021, 11:36 AM), https://perma.cc/B9WT-MU93 (explaining that Kosovo reached a verdict in 2021 on human rights abuses that took place in 1999).

[162] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 546 (D. Md. 2007).

[163] FED. R. EVID. 901(b)(4).

specific facts contained in a document.[164] A witness is not necessarily required to authenticate evidence under the distinctive-characteristics doctrine.[165] While many documents could theoretically fall under the distinctive-characteristics doctrine, one common example is an email chain.[166] Email chains are frequently admissible under Rule 901(b)(4) because they contain distinguishing information about a litigant: An email address often uses an individual's name, for example, and the body of the email may include the individual's nickname or other unique identifiers.[167]

Several aspects of hashing and DLT suggest that the distinctive-characteristics doctrine can apply to these technologies.[168] First, hash values themselves can be considered distinctive characteristics that fall under Rule 901(b)(4).[169] The hash is a unique identifier, which provides a document with distinctive "contents" or "characteristics" as required by the rule.[170] Second, the metadata preserved by DLT could be sufficiently distinctive to allow for authentication.[171] By hashing and uploading evidence to distributed

[164] *Id.* R. 901(b)(4) advisory committee's note to 1972 proposed rules ("The characteristics of the offered item itself, considered in the light of circumstances, afford authentication techniques in great variety."); *see* United States v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (upholding the authentication of an email based on the email address, the contents of the email, the presence of nicknames, and testimony about the defendant's subsequent conduct); United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (similar); *see also In re* F.P., 878 A.2d 91, 94-95 (Pa. Super. Ct. 2005) (holding that an instant-message transcript was properly authenticated based on the appellant's use of his first name and the transcript's content, which was confirmed by other witnesses).

[165] *See* Las Vegas Sands, LLC v. Nehme, 632 F.3d 526, 533 (9th Cir. 2011) (noting that "the district court applied an incorrect legal standard" when it required authentication by a "competent witness with personal knowledge," especially given that the evidence "could have been authenticated by review of [its] contents").

[166] *See Lorraine*, 241 F.R.D. at 546.

[167] *See Siddiqui*, 235 F.3d at 1322-23; *Safavian*, 435 F. Supp. 2d at 40.

[168] Hashing, for example, can help establish the final (or "legally operative") version of an electronic document when version control presents a challenge. *See, e.g.*, *Lorraine*, 241 F.R.D. at 547. DLT can then ensure that this final version is preserved for trial.

[169] *See id.* at 546-47.

[170] FED. R. EVID. 901(b)(4); *Lorraine*, 241 F.R.D. at 546-47.

[171] *See Lorraine*, 241 F.R.D. at 547-48 (explaining how metadata can be used to authenticate electronic evidence). A detailed description of metadata can be found in *The Sedona Guidelines*, a report on best practices for managing electronic records. Appendix F defines metadata as "information about a particular data set which describes how, when and by whom it was collected, created, accessed or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information)." THE SEDONA CONF. WORKING GRP. ON BEST PRACS. FOR ELEC. DOCUMENT RETENTION & PROD., THE SEDONA GUIDELINES: BEST PRACTICE GUIDELINES & COMMENTARY FOR MANAGING INFORMATION & RECORDS IN THE ELECTRONIC AGE app. F at 94 (2005). Appendix E further defines metadata to include "all the contextual,

footnote continued on next page

ledgers, human rights advocates can preserve the original metadata alongside the raw evidence rather than risking accidental file modification by uploading the content to YouTube or storing the record on a laptop. The unchanged metadata would enable a court to trust the underlying data set, ascertain the distinctive characteristics therein,[172] and deem evidence admissible on those grounds.[173]

4. Reply-letter doctrine

Finally, the reply-letter doctrine is a common law principle that can be understood as a particular application of the distinctive-characteristics rule. Under the reply-letter doctrine, a document can be authenticated based on evidence that it "was sent in reply to a previous communication."[174] In other words, if an initial communication received a reply, courts assume that the

processing, and use information needed to identify and certify the scope, authenticity, and integrity of active or archival electronic information or records." *Id.* app. E at 80. Examples of metadata include

> a file's name, a file's location (e.g., directory structure or pathname), file format or file type, file size, file dates (e.g., creation date, date of last data modification, date of last data access, date of last metadata modification), [and] file permissions (e.g., who can read the data, who can write to it, who can run it).

Id. app. E at 80 n.1. For additional discussion of metadata, see notes 57-59 and the accompanying text above.

[172] While one might be worried about the development of deepfake technology, concerns regarding altered evidence have always been present in the context of the distinctive-characteristics doctrine. *See, e.g.*, People v. Slusher, 844 P.2d 1222, 1229 (Colo. App. 1992) (finding a document to be inauthentic due to the possibility of tampering, despite the document being found on the defendant's computer). There is always a chance that someone has tampered with a file and introduced fake or misleading distinctive characteristics, but this has never categorically barred a distinctive-characteristics authentication under Rule 901(b)(4). *See, e.g.*, *In re* F.P., 878 A.2d 91, 94-95 (Pa. Super. Ct. 2005) (finding that an instant-message transcript was sufficiently authenticated despite the possibility that someone else logged in to the appellant's account). Instead, courts have looked for other corroborating evidence in addition to the distinctive characteristics of the proffered evidence. *Siddiqui*, 235 F.3d at 1322-23 (authenticating email evidence in part through indirect testimony). The same logic would apply here given the possibility of deepfakes.

[173] Verification, or the "process of establishing the [substantive] accuracy or validity of information that has been collected online," *Berkeley Protocol*, *supra* note 14, ¶ 176, is beyond the scope of this Note. But it is worth mentioning that the very nature of metadata could help verify evidence. Specifically, the date, time, and location information contained in metadata could confirm that a photo or video actually shows the event or atrocity in question. For example, if an attack occurs on March 4, 2019, at 2:17 AM in Manila and a video or photo is uploaded to a distributed ledger on March 4, 2019 at 2:22 AM from a location close to the attack, then a judge might reasonably conclude that the video depicts what it is purported to depict.

[174] Winel v. United States, 365 F.2d 646, 648 (8th Cir. 1966).

reply was sent by the intended recipient of that communication.[175] The reply-letter doctrine thus allows courts to use a response's content to both authenticate the response and attribute it to the responding party.

The reply-letter doctrine has evolved to apply to various forms of communication, including telegrams[176] and phone calls responding to letters.[177] As evidence law moves into the digital age, courts are beginning to extend this method of authentication to emails and social media posts.[178] Because courts have admitted messages sent over the internet where "the evidence establishes the identity of the sender,"[179] the reply-letter doctrine could help ensure admissibility in human rights cases where digital communications play a central role.[180] But some have raised concerns about extending the reply-letter doctrine beyond physical letters, fearing that the doctrine's underlying logic—that only the recipient of a correctly addressed letter is likely to have received and responded to it—breaks down in contexts where intermediaries in the transmission process can disrupt the integrity of the communication.[181]

There are two possible issues with using the reply-letter doctrine to authenticate digital communications: a *content-integrity* concern (that digital content can be manipulated after receipt in ways that physical letters cannot) and an *identity-integrity* concern (that it is easier to impersonate a respondent using a digital transmission process). Hashing and DLT mitigate concerns

[175] *See* 31 CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 7109 (West 2021).

[176] United States v. Weinstein, 762 F.2d 1522, 1533 (11th Cir.) ("[L]etters and presumably telegrams are prima facie authentic if their content is responsive to prior properly admitted communications."), *modified on denial of reh'g*, 778 F.2d 673 (11th Cir. 1985) (per curiam).

[177] Van Riper v. United States, 13 F.2d 961, 968 (2d Cir. 1926) ("If, for example, a man were to write a letter, properly addressed to another, and were to receive a telephone call in answer, professing to come from the addressee, and showing acquaintance with the contents of the letter, it would in our judgment be a good enough identification of the speaker to allow in the proof . . . .").

[178] *See* Varkonyi v. State, 276 S.W.3d 27, 35 (Tex. App. 2008); People v. Downin, 828 N.E.2d 341, 350-51 (Ill. App. Ct. 2005); State v. Hannah, 151 A.3d 99, 106-07 (N.J. Super. Ct. App. Div. 2016).

[179] Bloom v. Commonwealth, 542 S.E.2d 18, 20 (Va. Ct. App.), *aff'd*, 554 S.E.2d 84 (Va. 2001).

[180] *See, e.g.*, *supra* notes 1-3 and accompanying text.

[181] *See* 7 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2154, at 756-57 (James H. Chadbourn ed., 1978) (noting that reply telegrams are susceptible to forgery because they are not handwritten and require operators for transmission); 31 WRIGHT & MILLER, *supra* note 175, § 7109 (explaining that courts are reluctant to extend the reply-letter doctrine to instances where people other than the intended recipient could have seen the initial communication).

about manipulation, strengthening the case for using the reply-letter doctrine to authenticate digital evidence.

DLT and hashing can address the content-integrity concern by preserving the content of and data associated with a digital communication.[182] A human rights organization can hash a message and store it on a distributed ledger, essentially placing the message in a digital lockbox. A reply to the message (or the message itself, if it is a reply) can then be verified as authentic and unchanged, allowing courts to confidently conclude that it was not subject to digital manipulation during its receipt and storage.

Cryptographic tools can also help resolve the identity-integrity concern, albeit in more limited circumstances. The identity-integrity concern is rooted in the fact that unencrypted digital messages can be intercepted (and responses forged or hacked), making courts hesitant to assume that replies come from the intended recipient.[183] The use of encryption, a technique somewhat similar to hashing, helps solve this problem. While hashing is a "one-way function" meant to attach a unique fingerprint to a piece of information, encryption is a "two-way function" that uses cryptographic keys to scramble information when it is in transit and unscramble it upon proper receipt.[184] Thus, if a communication is sent using encryption, a court can comfortably presume that (1) a third party has not inappropriately seen the message; and (2) the replying party is the intended recipient of the initial inquiry.

Human rights advocates and others can obtain valuable evidence by intercepting unencrypted communications, however,[185] and the identity-

[182] Preserving location data is somewhat tricky: This data relies on a computer's IP address, which can be altered using fairly accessible software. *How IP Addresses Work on Google*, GOOGLE SEARCH HELP, https://perma.cc/RT5Q-ERCJ (archived Apr. 14, 2022); *How Do I Hide My IP Address?*, AVAST, https://perma.cc/X55T-WRDQ (archived Apr. 14, 2022); *see also* EUR. UNION AGENCY FOR CYBERSECURITY, PSEUDONYMISATION TECHNIQUES AND BEST PRACTICES: RECOMMENDATIONS ON SHAPING TECHNOLOGY ACCORDING TO DATA PROTECTION AND PRIVACY PROVISIONS 6-7, 27 (2019), https://perma.cc/7PZ4-JVUX (discussing advances in anonymization techniques and emphasizing anonymity's role in security and privacy).

[183] That said, the potential for hacking does not seem to categorically bar authentication under the reply-letter doctrine. *See, e.g.*, *Downin*, 828 N.E.2d at 350-51 (finding an email properly authenticated under the reply-letter doctrine despite the possibility of hacking or falsification). Instead, judges take this possibility into account when assessing authenticity. *See* People v. Kent, 81 N.E.3d 578, 595 (Ill. App. Ct. 2017) (finding Facebook messages inauthentic where the State did not adequately rule out the possibility that someone else was using the defendant's Facebook account). *See generally* United States v. Thomas, 701 F. App'x 414, 419 (6th Cir. 2017) (considering how to weigh hacking or fabrication when authenticating social media profile pictures).

[184] *Hashing vs Encryption—The Big Players of the Cyber Security World*, INFOSEC INSIGHTS (July 20, 2019), https://perma.cc/WMT8-MS6L.

[185] *See, e.g.*, Evan Hill & Christiaan Triebert, *12 Hours. 4 Syrian Hospitals Bombed. One Culprit: Russia.*, N.Y. TIMES (updated May 4, 2020), https://perma.cc/D22R-2HQN (describing

footnote continued on next page

integrity concern resurfaces for such communications. Indeed, when communications are easily intercepted, defendants can claim that anyone could have seen the initial inquiry and impersonated the intended recipient. Courts should feel confident extending the reply-letter doctrine to digital communications when identity and content issues are mitigated by technological safeguards, but this will realistically only be possible for a small amount of the digital evidence that human rights advocates seek to admit.

D. Best Options for Authenticating Digital Evidence Without Witnesses

Although a variety of doctrines and common law principles can be used to authenticate digital evidence stored using hashing and DLT, some doctrines apply more cleanly to such evidence than others. Self-authentication under Rule 902(14) is the most intuitive option for human rights activists using DLT and hashing. Unlike a common law principle that is subject to a large degree of judicial discretion, Rule 902(14) is codified in the Federal Rules of Evidence with commentary that sharpens its contours.[186] As such, it would benefit human rights defenders to take advantage of the rule, especially because it so clearly contemplates authentication via hash values. As noted above, however, the logic underlying Rule 902(14) presupposes a centralized business or organization that regularly hashes and stores information.[187] While exploring the specifics of a centralized distributed ledger for human rights evidence is beyond the scope of this Note, it is important to emphasize that such a ledger would be helpful in authenticating evidence under Rule 902(14). Beyond Rule 902(14), common law doctrines like chain of custody, silent witness, distinctive characteristics, and reply letter all provide avenues for authentication. Among these, the distinctive-characteristics doctrine may be the most attractive because metadata and hash values are generally unique to each record. On the other hand, the silent-witness theory and chain of custody may be less attractive because they require a more technical explanation or a step-by-step recounting of a record's whereabouts.

E. Vulnerabilities

While hashing and DLT hold immense promise, there are a handful of doctrinal and constitutional concerns that may caution against widespread authentication of digital evidence without witnesses. Ultimately, these concerns should not threaten the use of DLT and hashing to authenticate

how cockpit radio recordings allowed the *New York Times* to link specific wrongdoers to airstrikes on civilian targets).

[186] FED. R. EVID. 902(14); *id.* R. 902(14) advisory committee's note to 2017 amendment.

[187] *See supra* notes 122-27 and accompanying text.

digital evidence. Instead, they should be used to inform the proper application of these technologies.

1. Unsubstantiated collection or capture

One significant blind spot of any argument for admissibility predicated *only* on hashing and DLT is the failure to account for the moment of creation. While these technologies create a long-term storage process that is functionally ironclad, they can only safeguard digital evidence once it has been hashed and entered into the ledger. In other words, these technologies do not guarantee the reliability of evidence before the hash function is applied. This point has clear implications for authentication arguments relying on chain of custody and the silent-witness theory. Hashing and DLT do not automatically test whether data was altered prior to entry in the system: The period before hashing is thus unaccounted for, potentially creating a gap in the chain of custody or in the otherwise-reliable process that leads to silent-witness status. Concerns about this gap are especially trenchant in the human rights space, where data is often captured via unsophisticated means (such as a generic cell phone camera) and can remain in the hands of individuals without technical expertise for a long time. Moreover, some healthy skepticism of digital evidence may be appropriate in the internet age, where photos and videos can be manipulated or doctored prior to hashing.[188] The silent-witness jurisprudence regarding surveillance cameras may present a way forward: Evidence need not be flawlessly constituted to be authenticated. For example, courts have not always required independent evidence of a defendant's actions to supplement surveillance photographs,[189] and surveillance footage remains admissible even if there are gaps in the video.[190]

[188] *See* John P. LaMonaca, Comment, *A Break from Reality: Modernizing Authentication Standards for Digital Video Evidence in the Era of Deepfakes*, 69 AM. U. L. REV. 1945, 1976-77 (2020) (arguing that even eyewitness testimony may no longer be sufficient for authentication given advances in deepfake technology). Note, however, that this skepticism could disproportionately impact communities of color and marginalized communities, "whose stories society is already less likely to believe." *See* Riana Pfefferkorn, *The Threat Posed by Deepfakes to Marginalized Communities*, BROOKINGS: TECHSTREAM (Apr. 21, 2021), https://perma.cc/FQB3-9X8N.

[189] United States v. Taylor, 530 F.2d 639, 641-42 (5th Cir. 1976) (finding that indirect testimony "furnished sufficient authentication for the admission" of surveillance photographs under the silent-witness theory).

[190] People v. Taylor, 956 N.E.2d 431, 440 (Ill. 2011) (finding video evidence sufficient despite missing segments and a short recording time); 16 AM. JUR. 3D *Proof of Facts* § 27 (West 2022) ("[T]echnical difficulties . . . do not require automatic exclusion if the difficulties can be remedied or if the remaining portions of the videotape have sufficient probative value. The admissibility of imperfect or defective videotape evidence, and what, if anything, should be done to address the defect, is left to the trial court's discretion." (footnote omitted)).

Fortunately, litigants can anticipate and preempt reliability concerns. The most effective solution would be for human rights advocates to deploy an integrated system for collection and storage. If individuals collecting evidence could instantaneously hash and upload data to a distributed ledger after capture, hashing and DLT would combine to ensure a perfect chain of custody. Countless technology companies are engaged in the development of such integrated tools, with Truepic serving as a successful pioneer.[191] While well-resourced NGOs have begun to test systems like this in the field,[192] most human rights documentation is not subject to rigorous, automated capture processes. When evidence is not immediately hashed and stored upon its creation, a witness (or some other attestation as to the integrity of the chain of custody) may still be necessary to explain the period from capture to hashing and digital storage.

Even when there is a gap between capture and hashing, however, litigants can potentially validate evidence by submitting metadata—typically, a date, time, and location stamp—along with the evidence itself.[193] Indeed, courts have relied on date, time, and location information to help support authentication in the past.[194] This information can thus be used in the same way as a manager's testimony regarding the location of surveillance cameras inside a store.[195] Beyond metadata, other types of supplemental evidence could include (1) expert reports attesting to the photo or video's journey from capture to storage; or (2) additional photos or videos contextualizing the evidence in question. If there is residual doubt as to the evidence's validity, that doubt

[191] Mike Freeman, *San Diego's Truepic Pulls In $26M with Backing from Microsoft to Fight "Deep Fakes,"* SAN DIEGO UNION-TRIB. (Sept. 15, 2021, 5:39 PM PT), https://perma.cc/7MME-B5PP; *see also Our Technology, supra* note 89.

[192] *See, e.g.*, *Our Work*, MNEMONIC, https://perma.cc/EQ6L-GNTA (archived Dec. 30, 2021) ("Mnemonic builds and supports the development of tools to increase human right's [sic] defenders['] capacity to use digital information to advance social justice."); *Our Work*, WITNESS, https://perma.cc/N5PE-WMQA (archived Dec. 30, 2021) ("WITNESS identifies ways for citizens to capture and preserve footage to improve its chances of . . . being used in the courtroom.").

[193] *See* People v. Goldsmith, 326 P.3d 239, 245 (Cal. 2014) (noting that the foundation for authentication "may be supplied by other witness testimony, circumstantial evidence, content and location"). In modern devices like mobile phones, "[d]etails about when, where, and how a photo was taken are captured automatically" and included in photograph metadata. Thomas Germain, *How a Photo's Hidden "Exif" Data Exposes Your Personal Information*, CONSUMER REPS. (updated Dec. 6, 2019), https://perma.cc/MM93-2YJY; *see supra* note 58 and accompanying text (defining metadata); *supra* note 171 (same).

[194] *See, e.g.*, United States v. Rembert, 863 F.2d 1023, 1028 (D.C. Cir. 1988) (finding that a film's "internal indicia" of date and location helped "provide ample support" for authentication).

[195] *See supra* note 160 and accompanying text.

should be reflected in the weight that the jury affords the evidence rather than a general bar on its admission.[196]

2. Hearsay and the constitutional right to confrontation

Ensuring the reliability of digital evidence is particularly important in light of U.S. evidence law's concern with hearsay.[197] The prohibition against hearsay captures a seemingly simple preference for testimony under oath that can be observed by the jury and is subject to cross-examination.[198] When a party introduces out-of-court statements "to prove the truth of the matter asserted," those statements are generally inadmissible hearsay.[199] While simple on its face, the hearsay rule has developed into a complex web of widely criticized[200] provisions replete with carveouts and exceptions.[201]

A full explanation of the nexus between hearsay and digital human rights evidence is beyond the scope of this Note. That is because hearsay considerations revolve around the nature of the evidence—what it shows and what it is being offered to prove—rather than its authenticity. For example, imagine a video of soldiers attributing blame to their commander for intentional attacks on civilians. If the commander is later sued and challenges the video as inadmissible hearsay, the use of hashing and DLT will be irrelevant to the judge's hearsay determination. Her analysis will instead turn on the content of the video (what is being said, by whom, and in what circumstances) and potential hearsay exceptions.

Still, hearsay-like considerations arise in a narrow, serious context that carries constitutional weight. The Sixth Amendment guarantees a criminal defendant the right to be "confronted with the witnesses against him."[202] Although this bar on out-of-court testimony does not map cleanly onto

[196] *See* United States v. Fluker, 698 F.3d 988, 999 (7th Cir. 2012).

[197] *See* Steven W. Teppler, *Digital Data as Hearsay*, 6 DIGIT. EVIDENCE & ELEC. SIGNATURE L. REV. 7, 12-13 (2009) (noting that judges have difficulty applying hearsay rules to digital evidence).

[198] *See* David Alan Sklansky, *Hearsay's Last Hurrah*, 2009 SUP. CT. REV. 1, 15-16 (explaining how the "canonical story" justifying the hearsay rule contemplates "three safeguards: the oath the witness takes to tell the truth, the jury's ability to watch the witness's demeanor, and the opportunity for cross-examination").

[199] *See* FED. R. EVID. 801(c), 802.

[200] *See* Sklansky, *supra* note 198, at 1-2 (detailing various rationales for the hearsay rule's unpopularity).

[201] FED. R. EVID. 801(d), 802-804, 807.

[202] U.S. CONST. amend. VI. Some scholars believe that this right emerged from the Framers' "preoccupation with . . . ex parte affidavits," which were common evidentiary tools at the time of the Founding. Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 2041-42 (2017).

evidence created or stored by machines,[203] replacing live, in-person testimony with digital evidence may run afoul of the so-called Confrontation Clause. Specifically, a Confrontation Clause issue could arise if a judge perceives data collection and storage to be sufficiently similar to testimonial evidence. If data is so inscrutable as to be impervious to courtroom probing, the argument goes, then a defendant's Sixth Amendment rights are infringed.[204] This argument grows stronger as police and prosecutors deploy sophisticated and opaque technologies in the pursuit of carceral outcomes.[205]

While Confrontation Clause concerns may hold water for complex algorithms or machine-learning systems,[206] hashing and DLT do not raise constitutional issues on their own. The processes behind these technologies are distinct from the evidence in question; DLT and hashing simply safeguard the actual probative material, as would an evidence locker. These technologies do not generate, interfere with, or complicate the underlying data. Accordingly, hashing and DLT do not exacerbate concerns that defendants will be unable to "confront" digital evidence.

To the extent that hashing and DLT are used in conjunction with testimonial evidence (including data), the Supreme Court has implied that process-based evidence can be admissible when accompanied by testimony from individuals involved with the underlying process.[207] To satisfy the Confrontation Clause in such cases, courts may require representatives from human rights organizations to testify to their use of hashing and DLT. But as discussed in Part II above, hashing and DLT are readily decipherable concepts: Litigants should have no problem explaining these technologies to judges and

[203] Indeed, courts have struggled to shoehorn digital or process-based evidence into a witness-centric evidentiary regime. *See* Roth, *supra* note 202, at 2006 (describing the "patchwork of ill-fitting hearsay exceptions, confusing authenticity rules, and promising but inadequate reliability requirements for expert methodologies" applied to "machine testimony"); Cheng & Nunn, *supra* note 13, at 1110-12 (arguing that requiring live witness testimony for process-based evidence is an "empty shell" when it comes to protecting a defendant under the Confrontation Clause).

[204] *See* Roth, *supra* note 202, at 2042-43 (noting that complex processes can threaten the rights of the accused when there is no way to test their credibility).

[205] Even given this shift, "many courts have surrendered their gatekeeping role for machine accusers and are not enforcing evidentiary rules." Brian Sites, *The Future of the Confrontation Clause: Semiautonomous and Autonomous Machine Witnesses*, 22 VAND. J. ENT. & TECH. L. 547, 549 (2020).

[206] *See* Roth, *supra* note 202, at 2043-44.

[207] *See, e.g.*, Melendez-Diaz v. Massachusetts, 557 U.S. 305, 311 (2009) (holding that a defendant's right to confrontation was violated when certificates of forensic evidence were presented at trial without testimony from the forensic analysts); Bullcoming v. New Mexico, 564 U.S. 647, 652 (2011) (holding that in-court surrogate testimony for a forensic report provided by "a scientist who did not sign the certification or perform or observe the test" violated the Confrontation Clause).

juries. Furthermore, Confrontation Clause jurisprudence has emphasized the importance of reliability,[208] and litigants can use hashing and DLT to increase reliability by showing the lifecycle of data from the moment it is hashed and stored to the moment it appears in court.[209] In sum, while hashing and DLT alone should not trigger constitutional concerns, the use of these technologies alongside testimonial evidence could implicate the Confrontation Clause and require specific witness testimony regarding functionality.

3. The continued importance of live witness testimony

Reliance on digital evidence in place of witness testimony can produce adverse consequences at trial. First, as human rights advocates increasingly rely on sophisticated technologies to collect and store evidence, they must become adept at defending the legitimacy of those technologies in court. Defendants challenging digital evidence may also seek access to the underlying design and code of the relevant computer programs.[210] Both these things create problems for companies and NGOs. Because human rights advocates are generally not technologists, fighting challenges to hashing and DLT could cost substantial time and money (through legal research, expert testimony, and so on), especially at first. In addition, such challenges could expose proprietary information, revealing key evidence-collection methods to human rights abusers.

Second, heavy use of video or digital evidence may distort jury or factfinder perceptions. Courts have historically been lenient in assuming the credibility and impartiality of electronic evidence.[211] Once admitted, this evidence can "lead[] perceivers to evaluate [photos or] video with a naïve realism" that can "disincline perceivers to question how the images were constructed and what information is excluded from the display."[212] Legal

[208] *See* Crawford v. Washington, 541 U.S. 36, 61 (2004) (emphasizing that "the Clause's ultimate goal is to ensure reliability of evidence").

[209] *See supra* Parts II, III.C.1.

[210] *Cf.* State v. Chun, 943 A.2d 114, 170 (N.J. 2008) (requiring a developer to produce the source code used in software to detect blood-alcohol levels).

[211] *See* Sergey Bratus, Ashlyn Lembree & Anna Shubina, *Software on the Witness Stand: What Should It Take for Us to Trust It?*, *in* TRUST AND TRUSTWORTHY COMPUTING 396, 409 (Alessandro Acquisti, Sean W. Smith & Ahmad-Reza Sadeghi eds., 2010) ("A review of cases admitting evidence and expert testimony based on evidence reveals that distrust of the machines used to create evidence and the software running on these machines is a fairly rare commodity, despite technical challenges to accuracy of such machines and their source code.").

[212] Yael Granot, Emily Balcetis, Neal Feigenson & Tom Tyler, *In the Eyes of the Law: Perception Versus Reality in Appraisals of Video Evidence*, 24 PSYCH. PUB. POL'Y & L. 93, 94 (2018) (emphasis omitted).

scholarship has emphasized the concept of perspective bias, or the power of camera positioning to influence jury responses to recorded confessions.[213] But distortionary concerns can also apply in the human rights context. For example, if a judge is only exposed to photographs of an atrocity, her understanding of the context may be limited and her judgment accordingly affected. Judges unaccustomed to working with data may not even take the time to engage with digital evidence absent direction from live witnesses.

Third, victim participation has often been a hallmark of the justice process for cases related to human rights abuses and atrocities.[214] Without the emotional heft of live testimony, digital evidence might inadequately convey the devastation of an event or appear to substitute sterile, forensic data for victims' experiences. Beyond efficacy concerns, complete reliance on digital evidence would deny victims the empowering opportunity to articulate their experiences and take ownership over the conflict narrative in the context of transitional justice.

* * *

Given the above vulnerabilities, litigants will need to be both creative and cautious when trying to authenticate digital evidence using the doctrines covered in this Part. But putting these vulnerabilities aside, DLT and hashing provide a superior method of storage—and one that more easily maps onto existing evidentiary rules—than current unregulated storage techniques. DLT and hashing ensure the general immutability of digital evidence, giving evidence stored using these technologies a comparative advantage over evidence stored on a computer hard drive or a hosting site like YouTube.[215]

IV. Considerations for Judges, Juries, and Human Rights Organizations

Litigants and jurists alike should take a balanced approach when reviewing evidence preserved using hashing and DLT. Judges in particular should act as vigilant gatekeepers, admitting only reliable evidence and properly instructing juries on the underlying technologies. Meanwhile, human rights organizations should mindfully design their technical systems to overcome evidentiary hurdles. While additional measures can and should be taken to ensure the validity of proffered digital evidence, lack of direct witness testimony alone should not stop admission at the courthouse doors.

[213] *See, e.g.*, Aaron M. Williams, Note, *The Noisy "Silent Witness": The Misperception and Misuse of Criminal Video Evidence*, 94 IND. L.J. 1651, 1658-64 (2019).

[214] *See* Elisabeth Baumgartner, *Aspects of Victim Participation in the Proceedings of the International Criminal Court*, 90 INT'L REV. RED CROSS 409, 410 (2008).

[215] *See, e.g.*, Rosen, *supra* note 34.

A. Guidelines for Judges and Juries

Foundational requirements regarding soundness of technical process should guide judicial thinking about hashing and DLT.[216] Several such requirements are relevant to authenticity regardless of how the litigant seeks to admit digital evidence.

First, judges should seek operational evidence on (1) how hashing and DLT protect against alterations; and (2) where these technologies are vulnerable. Digital evidence is uniquely susceptible to alterations that are undetectable to the untrained eye, so judges should request supplemental evidence on procedural safeguards for the data in question. This is already common practice for photos taken by automatic cameras,[217] and such supplemental evidence can aid discretionary decisionmaking by giving judges a clear understanding of the ways in which hashing and DLT can (and cannot) prevent unwanted manipulation. This evidence would also enable opposing counsel to raise counterarguments, helping courts effectively weigh and address the concerns raised in Part III.E above.

[216] Courts have previously used foundational requirements to inform the evidentiary treatment of new technologies. *See* People v. Taylor, 956 N.E.2d 431, 438 (Ill. 2011) (referring to the "foundational requirements" used to establish "the accuracy of a process that produces surveillance camera recordings"). Foundational requirements have included system reliability and operation (including competency of the operator, if applicable), the handling and safeguarding of footage before trial, and evidence regarding the possibility of tampering. *See* United States v. Harris, 55 M.J. 433, 439 (C.A.A.F. 2001) (determining that "the record establishes a reasonable foundation for authenticating . . . photos taken by [an] automated camera" because "(1) the system was reliable; (2) the system was in working order when the photo was taken; and (3) the film was handled and safeguarded properly from the time it was removed from the camera until the time of trial"); United States v. Biggins, 551 F.2d 64, 66 (5th Cir. 1977) (considering four foundational factors for a recording in a criminal case: "the competency of the operator, the fidelity of the recording equipment, the absence of material deletions, additions, or alterations in the relevant portions of the recording, and the identification of the relevant speakers"). Even where foundational requirements are generally used, a judge's discretion is preserved through the opportunity for case-by-case analysis. *See* United States v. Reed, 887 F.2d 1398, 1405 (11th Cir. 1989) ("Although the preferred practice is for the government to produce evidence regarding the competence of the tape machine operator, fidelity of the equipment, the absence of alterations to the tape and the identity of the speakers, the trial court has broad discretion to allow tapes into evidence without such a showing so long as there is independent evidence of accuracy.").

[217] *See, e.g.*, United States v. Gray, 531 F.2d 933, 935 (8th Cir. 1976) (per curiam) (holding that testimony describing the operation of a Regiscope, an automated system used to validate checks, established sufficient foundation for the admission of a fraudulent-check photograph); Ferguson v. Commonwealth, 187 S.E.2d 189, 191 (Va. 1972) (finding testimony regarding Regiscope reliability to be "sufficient to provide an adequate foundation assuring the accuracy of the process" and holding that a photograph was "properly admitted in evidence").

Second, judges should require data on error rates for the specific hashing algorithm and distributed ledger used.[218] This idea is already expressed through the *Daubert* rule, which ensures that an expert witness's scientific testimony is "based on scientifically valid principles" that can properly be applied to the facts at issue.[219] Although courts apply the *Daubert* rule to scientific evidence, its logic could readily extend to technologies such as hashing and DLT.[220] Though error-rate data would not perfectly capture the accuracy of a photo or video, it would at least ensure that the parties have the information needed to assess whether the technology at issue adequately protects evidence from manipulation.[221]

Third, judges should require litigants to show the entire chain of custody for digital evidence, particularly the links in the chain before the evidence was hashed and stored on a distributed ledger. The gap between capturing a photo and hashing and storing it—even if it lasts only a few minutes—provides a time frame during which the photo could have been altered or manipulated. Because hashing does not say anything about the reliability of evidence before it is hashed, judges and defense counsel alike would benefit from knowing the hashing and storage timeline to assess the likelihood that an alteration may have taken place.

Fourth, any digital evidence submitted should include supplemental information about the storage host. Ideally such evidence would include the host's (1) mission; (2) leadership team; (3) technical expertise; (4) funding streams; (5) technologies used to protect against manipulation; and (6) policies in place to guard against illicit alterations by staff. Such information would assist judges in assessing whether the host itself is a trustworthy custodian.

Fifth and finally, judges should require independent confirmation of the object or event captured by a photo or video. This can be done in two ways. First, judges can consider date, time, and location evidence taken from metadata that was also hashed and stored using DLT. This information can be cross-checked with details regarding the purported object or event. Second, judges can look to supplemental evidence to confirm what the photo or video

[218] *Cf.* Munia Jabbar, Note, *Overcoming* Daubert*'s Shortcomings in Criminal Trials: Making the Error Rate the Primary Factor in* Daubert*'s Validity Inquiry*, 85 N.Y.U. L. REV. 2034, 2054 (2010) ("The lower the error rate of a scientific methodology, the more likely the methodology is accurate, and thus the more likely that it provides probative evidence. The error rate is therefore a concrete and objective way to measure the probative value of evidence." (footnote omitted)).

[219] Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 592-95, 597 (1993).

[220] *See* Cheng & Nunn, *supra* note 13, at 1114 (pointing to error rates as one way to ensure the reliability of process-based evidence under *Daubert*).

[221] Error recognition is particularly important because, as may be expected, not all programs are error free. *See, e.g.*, *supra* Part II.A.1 (explaining the risk of hash collisions).

purportedly depicts.[222] For example, if the proffered photo shows a religious site that was allegedly targeted in an airstrike, the judge could require additional photos of the site taken prior to the incident to cross-check visual points of reference before and after the strike.

After evidence has been properly admitted, juries may lack the technical expertise to properly weigh digital evidence that is hashed and stored using DLT. If such evidence is submitted without witness testimony, judges should instruct juries on how these technologies work and what their potential flaws are.[223] Juries should also be instructed on the limited perspectives that individual photos or videos provide: They are not omniscient representations of reality, but instead show reality from a single perspective. This instruction is particularly important when a photographer or videographer cannot be cross-examined before the jury. Such guidance would help close the technical gap, ensuring that hashing and DLT serve as aids for admissibility without becoming unfairly prejudicial.

B. Considerations for Human Rights Organizations and Litigants

Human rights organizations hoping to bring cases that rely on digital evidence would be wise to modify their storage practices in light of U.S. evidentiary standards. First, human rights organizations collecting digital evidence should deploy hashing as soon as possible by investing in the required technology and hiring the necessary staff. Once deployed, hashing should be performed as close to the time of capture as possible. The longer the window between capturing evidence and hashing it, the more latitude there is to question its validity.[224] Should there be multiple days between the time a photo was taken and the time it was hashed, for example, there are few avenues apart from witness testimony to establish that the photo was not manipulated.

Second, and more importantly, human rights organizations should work together to centralize digital evidence storage in a single hosting organization.

[222] For a model of this approach outside the courtroom, see Hill & Triebert, *supra* note 185 (explaining how reporters used flight logs, radio transmissions, videos, maps, and interviews to corroborate evidence of aerial attacks); Christiaan Triebert, Evan Hill, Malachy Browne, Whitney Hurst, Dmitriy Khavin & Masha Froliak, *How Times Reporters Proved Russia Bombed Syrian Hospitals*, N.Y. TIMES (updated Apr. 7, 2020), https://perma.cc/D743-FH5Y (discussing the reporters' use of geolocation, a method that relies on landmarks and geographical features to "determine the exact site of a photo or video"); and *The Attack on the Kafranbel Surgical Hospital*, SYRIAN ARCHIVE (June 26, 2019), https://perma.cc/HGP5-3PZ8 (describing how photos and videos served to verify an alleged airstrike).

[223] *See* Roth, *supra* note 202, at 2038 (suggesting that courts can avoid "black box dangers" by informing juries of how machines work and their potential problem points).

[224] *See supra* Part III.E.1.

Ideally this would be a collaborative effort to establish an integrated "storage locker," allowing each organization to submit digital evidence to a single distributed ledger.[225] A trusted, centralized host may enable the admission of evidence under Rule 902(14), which conceptualizes storage based on regular, businesslike practices.[226] Such a host could also mitigate concerns that the ledger's operator is unreliable (or dishonest) and lower the individual cost of collecting digital evidence.[227]

Widespread adoption of hashing and DLT may suffer from a range of logistical and pragmatic difficulties. For nonprofits operating with lean staffs and limited technical expertise, proper data protection is logistically daunting, especially when simplistic and (seemingly) secure systems like cloud storage exist.[228] And particularly without a centralized host, NGOs seeking to utilize DLT and hashing would require long-term storage capacity to handle massive amounts of data collected from a wide range of sources. Preserving evidence for litigation may also be subsidiary to other NGO aims such as awareness raising, advocacy, and humanitarian relief. Additionally, as technology evolves and documenters consider utilizing new platforms, the sunsetting of tools raises challenges regarding data transfer and interoperability. The above barriers may force NGOs and documenters to make difficult tradeoffs between security and usability, as well as between flexibility and structure.[229] Finally, there is the problem of overreliance on unverified data. If NGOs or other collectors of digital evidence cannot be sure of the data's veracity before hashing it and storing it on a ledger, they risk imbuing falsified evidence with a sense of legitimacy.[230] This risk makes it all the more important for human

[225] Although early hashing is better for purposes of authentication, *see supra* Part III.E.1, the host could hash the evidence on receipt if necessary.

[226] *See supra* Part III.B.

[227] It is not clear whether a centralized distributed ledger should be public or private; technologists and relevant stakeholders are likely best suited to make this determination. *See* DESHPANDE ET AL., *supra* note 63, at 3 (describing the pros and cons of public and private distributed ledgers). In any case, an impartial and reliable host for such a ledger could help avoid foul play and judicial mistrust.

[228] *See* PILPG, THE ENGINE ROOM & HURIDOCS, HUMAN RIGHTS DOCUMENTATION BY CIVIL SOCIETY—TECHNOLOGICAL NEEDS, CHALLENGES, AND WORKFLOWS 39-43 (2020), https://perma.cc/P786-WARB (highlighting the evidentiary challenges that transitional-justice experts face when working with civil-society documenters).

[229] *See id.* at 67-69.

[230] This is where alarming narratives around the dangers of deepfakes bubble up. The term "deepfake" has come to describe any convincing alteration to a piece of digital content, and while the risk of data corruption or manipulation is serious, popular imagination has largely outrun the scope of the threat. For a lucid, measured examination of the scope of the problem, see generally WITNESS, *supra* note 69. For a more speculative (and slightly more pessimistic) assessment, see Riana Pfefferkorn, *"Deepfakes" in the Courtroom*, 29 B.U. PUB. INT. L.J. 245, 270-71 (2020) (positioning

footnote continued on next page

rights organizations to be judicious about what evidence, whether generated internally or by outside observers, is hashed and stored using DLT.

Despite these concerns, it is clear that human rights organizations should prioritize the implementation of DLT and hashing. This is especially true given the promise of these technologies for preserving evidence of human rights violations and admitting this evidence without witness testimony where necessary.

Conclusion

As the D.C. Circuit observed in 1988, technology does not stand still, and neither should the law.[231] In our modern digital era, virtually any person with a smartphone or recording device can document human rights abuses. Indeed, many have done so.[232] As a result, human rights organizations in the United States and around the world are beginning to collect this data, including photos, videos, and digital communications, with an eye toward eventual accountability proceedings.[233] Hashing and DLT have become essential tools in this pursuit: They safely and reliably store terabytes of data collected by trained observers, journalists, and everyday citizens reporting abuses.[234] Hashing and DLT also provide solutions to evidentiary problems associated with diffuse digital capture in human rights litigation. Because these technologies protect photos and videos from manipulation in a transparent manner, a lack of corroborative witness testimony and questions about authenticity should not necessarily bar admission of digital evidence at trial. While DLT and hashing may raise constitutional and prudential concerns, we conclude that judges and juries alike can take appropriate measures to mitigate

deepfake technology's ramifications for the legal field as hypothetical but looming). *See also* William Sasse, *Deepfakes and the Courtroom*, 2 MD. BAR J., no. 2, 2020, at 88, 89 ("[T]here may come a day when [deepfakes] threaten the legitimacy of our justice system."); Rob Toews, *Deepfakes Are Going to Wreak Havoc on Society. We Are Not Prepared.*, FORBES (May 25, 2020, 11:54 PM EDT), https://perma.cc/S4JY-MA9M (predicting the development of mass distrust as deepfake technology proliferates); Karen Hao & Will Douglas Heaven, *The Year Deepfakes Went Mainstream*, MIT TECH. REV. (Dec. 24, 2020), https://perma.cc/77JK-CCDN (highlighting multiple applications of deepfake technology); Danielle C. Breen, Note, *Silent No More: How Deepfakes Will Force Courts to Reconsider Video Admission Standards*, 21 J. HIGH TECH. L. 122, 125-26 (2021) (describing the threat that deepfake technology could pose to courtroom proceedings).

[231] *See* United States v. Rembert, 863 F.2d 1023, 1027 (D.C. Cir. 1988).

[232] *See* Brianne McGonigle Leyh, *Changing Landscapes in Documentation Efforts: Civil Society Documentation of Serious Human Rights Violations*, 33 UTRECHT J. INT'L & EUR. L. (PUB. INT'L L. & POL'Y) 44, 48 (2017).

[233] *See id.* at 45-48.

[234] *See supra* Part II.B.

adverse effects. Human rights organizations can further limit concerns by developing best practices and collaborating to create a trusted ledger.

Ultimately, this Note's analysis matters not only because the law should keep up with technology, but also because the rapid expansion of technology presents an opportunity to democratize accountability. As millions of people gain the ability to document human rights abuses in real time, perpetrators should no longer be able to act with impunity. Hashing and DLT can contribute to this accountability project—with potentially profound implications for international justice. Courts would be wise to authenticate digital evidence not just because new technologies make it possible, but because democratic pressures on our justice system demand it.